Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Data Breach Reporting Requirements	)	WC Docket No. 22-21
	)	

REPORT AND ORDER

Adopted: December 13, 2023 **Released: December 21, 2023**

By the Commission: Chairwoman Rosenworcel and Commissioners Starks and Gomez issuing separate statements; Commissioners Carr and Simington dissenting and issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION

1. Americans should have confidence that when they use communications services, their personal information is protected. These services are a ubiquitous feature of modern life, and they provide a vital lifeline for consumers. In providing these critical services, telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) providers often collect large quantities of sensitive customer data. Information such as records of the telephone numbers a person has called, or mobile phone location data showing the places they have been, can provide insights into medical conditions, religious beliefs, personal associations, and many other aspects of an individual's private life.[1]

2. The Commission's breach notification rule provides an important protection against improper use or disclosure of customer data, helping to ensure that carriers[2] are held accountable and providing customers with the tools to protect themselves in the event that their data is compromised. However, in the 16 years since the Commission adopted its data breach reporting rule—designed to protect customers against the threat of "pretexting"[3]—data breaches have only grown in frequency and severity.[4]

3. Telecommunications companies may be particularly vulnerable to these attacks.[5] In response to these evolving threats, today we update the Commission's rule regarding data breach notifications. Because consumers may be harmed by the improper use or disclosure of sensitive customer

[1] *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018) ("A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."); *id*. at 2217 (cell phone location data "provides an intimate window into a person's life" revealing not only physical movements, but "familial, political, professional, religious, and sexual associations.").

[2] As in the *Data Breach Notice*, in this Order we refer to telecommunications carriers and interconnected VoIP providers collectively as "telecommunications carriers" or "carriers," consistent with our existing Part 64, Subpart U rules. *See Data Breach Reporting Requirements*, WC Docket No. 22-21, Notice of Proposed Rulemaking, FCC 22-102, 3, para. 3 n.12 (2023) (*Data Breach Notice*). In doing so, we do not address the regulatory classification of interconnected VoIP service or interconnected VoIP service providers. *See* 47 CFR § 64.2003(o) (defining *telecommunications carrier* or *carrier* for purposes of Subpart U to include an entity that provides interconnected VoIP service as that term is defined in 47 CFR § 9.3).

[3] Pretexting is a practice in which a scammer pretends to be a particular customer or other authorized person in order to obtain access to that customer's call detail or other private communications records. *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6928, paras. 1-2 & n.1. (2007) (*2007 CPNI Order*); 47 CFR § 64.2011.

[4] According to an IBM report, the global average cost of a data breach has increased 15% over the last three years. *See* IBM, *Cost of a Data Breach Report 2023*, https://www.ibm.com/reports/data-breach (last visited Oct. 25, 2023); *see also* Confidentiality Coalition Comments at 1 (reporting a 118% increase from 2020 to 2021 in unauthorized access incidents, and a 44% increase in ransomware attacks impacting publicly traded companies).

[5] *See, e.g.*, Sam Sabin, *Wave of Telecom Data Breaches Highlight Industry's Weaknesses*, Axios (Mar. 17, 2023), https://www.axios.com/2023/03/17/telecom-data-breaches-t-mobile-att; Dan Goodin, *T-Mobile Discloses 2nd Data Breach of 2023, This One Leaking Account PINs and More* (May 1, 2023), https://arstechnica.com/information-technology/2023/05/t-mobile-discloses-2nd-data-breach-of-2023-this-one-leaking-account-pins-and-more/ (reporting that T-Mobile experienced breaches of its customers' data every year between 2018 and 2023, including a 2023 breach impacting 37 million customers); Catherine Reed, *Verizon Data Breaches: Full Timeline Through 2023*, Firewall Times (Oct. 5, 2023), https://firewalltimes.com/verizon-data-breaches (describing Verizon's data breach experienced earlier this year, which exposed the data of 7.5 million subscribers); Monica Alleven, *AT&T Alerts 9M Wireless Customers of Security Breach*, Fierce Wireless (Mar. 10, 2023), https://www.fiercewireless.com/security/att-informs-9m-wireless-customers-security-breach (noting how AT&T informed 9 million wireless customers that an unauthorized person accessed their customer proprietary network information (CPNI) through a vendor's system).

data other than CPNI, we expand the scope of our breach notification rules to cover various categories of personally identifiable information (PII) that carriers hold with respect to their customers.[6] We also adopt the Commission's proposal to expand the definition of "breach" for both telecommunications carriers and telecommunications relay service (TRS) providers to include inadvertent disclosures of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier or TRS provider, and such information is not used improperly or further disclosed. As proposed, we require carriers and TRS providers to notify the Commission of breaches, in addition to the United States Secret Service (Secret Service) and Federal Bureau of Investigation (FBI). We require such notice to be made as soon as practicable, and in no event later than seven business days, after reasonable determination of the breach.

4. In order to limit the potential burdens on carriers, TRS providers, and consumers from notifications that are unlikely to require protective action, we eliminate the requirement to notify customers of a breach in those instances where a carrier or TRS provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. And, to further support consumers' ability to act quickly to protect themselves following a breach for which there is a risk of harm, we eliminate the mandatory waiting period for carriers to notify customers, and instead require carriers and TRS providers to notify customers of breaches of covered data without unreasonable delay after notification to the Commission and law enforcement, and no later than 30 days after reasonable determination of a breach, unless a delay is requested by law enforcement. As discussed below, we find that these changes will better protect consumers from improper use or disclosure of their customer information and harmonize our rules with new approaches to protecting the public already deployed by our partners in federal and state government.

II. BACKGROUND

5. *Section 222 and Privacy of Telecommunications Customer Information.* Section 222 of the Communications Act of 1934, as amended (Communications Act or Act) requires telecommunications carriers to protect the confidentiality of customer information that they receive or have access to by virtue of their provision of a telecommunications service.[7] Section 222(a) requires carriers to protect the confidentiality of "proprietary information" of, and relating to, their customers.[8] Pursuant to section 222(c)(1), a carrier that receives CPNI by virtue of its provision of a telecommunications service may only use, disclose, or permit access to that information in limited circumstances: (1) if it is required by law; (2) with the customer's approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service,[9] subject to certain exceptions.[10] The Act defines CPNI as "(A) information

[6] *See* 47 U.S.C. § 222(a) (imposing a duty on carriers to protect "proprietary information" of customers, among other entities). For the purposes of this Report and Order and the rules adopted herein, we use the term "covered data" to refer collectively to both PII and CPNI. *See also* Appx. A.

[7] 47 U.S.C. § 222. *See also Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, et al.*, CC Docket Nos. 96-115 et al., Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14419-20, paras. 12-14 (1999) (*1999 CPNI Reconsideration Order*).

[8] 47 U.S.C. § 222(a); *see also TerraCom, Inc. and YourTel America, Inc.*; *Apparent Liability for Forfeiture*, File No. EB-TCD-13-00009175, NAL/Acct. No. 201432170015, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13330, para. 13 (2014) (*TerraCom NAL*). Section 222(b) provides that a carrier that receives or obtains proprietary information from other carriers in order to provide a telecommunications service may only use such information for that purpose and may not use that information for its own marketing efforts. 47 U.S.C. § 222(b).

[9] 47 U.S.C. § 222(c)(1).

[10] Section 222(d) delineates certain exceptions to the general principle of confidentiality, including, among other provisions, those permitting a carrier to use, disclose, or permit access to CPNI obtained from its customers to protect the rights or property of the carrier, or to protect telecommunications services users "from fraudulent,

(continued….)

that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[11]

6. While the Commission has not and does not here articulate an exhaustive list of information that is CPNI, the Commission has determined that in practical terms, CPNI includes personally identifiable information derived from a customer's relationship with a provider of telecommunications services,[12] such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.[13] Information collected by a customer's device, such as lists of numbers called and calls received, and the locations from which calls have been made, is also considered CPNI when the collection is undertaken at the carrier's direction and the carrier has access to or control over the information.[14] In 2020, the Commission concluded in a Notice of Apparent Liability for Forfeiture and Admonishment that CPNI also includes customer location information derived by or made available to a carrier from the wireless mobile device of a customer regardless of whether the information was generated in connection with a call.[15] However, some types of sensitive data, such as a customer's name, address, and telephone number, are not considered CPNI.[16]

7. The Commission adopted its first rules to implement section 222 in 1998.[17] These initial rules established restrictions on telecommunications carriers' use and disclosure of CPNI, as well as a framework to require carriers to take effective steps to protect CPNI.[18] Under these rules, the Commission adopted safeguards such as requiring carriers to train their personnel on when they are and are not authorized to use CPNI[19] and to maintain records that track access to CPNI,[20] among other things.

(Continued from previous page)
abusive, or unlawful use" of telecommunications services. *Id.* § 222(d)(2). Section 222(d)(4) also authorizes certain uses of call location information in emergency situations, such as delivery to a public safety answering point for delivery of emergency services. *Id.* § 222(d)(4). Section 222(f) provides that for purposes of section 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to call location information concerning the user of a commercial mobile service other than in accordance with subsection (d)(4). *Id.* § 222(f).

[11] *Id.* § 222(h)(1).

[12] *2007 CPNI Order* at 6928, para. 1 n.2.

[13] *Id.* at 6930, para. 5.

[14] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Declaratory Ruling, 28 FCC Rcd 9609, 9609-10, paras. 2-4 (2013) (*2013 CPNI Declaratory Ruling*).

[15] *AT&T, Inc.*, File No.: EB-TCD-18-00027704, Notice of Apparently Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1757, paras. 33-35 (2020).

[16] *1999 CPNI Reconsideration Order*, 14 FCC Rcd at 14486-88, paras. 145-47 (adopting the conclusions of the Common Carrier Bureau that customer names, addresses, and telephone numbers are not CPNI).

[17] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information et al.*, CC Docket No. 96-115 et al., Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061 (1998) (*1998 CPNI Order*).

[18] *Id.* at 8195, para. 193.

[19] 47 CFR § 64.2009(b); *see also 1998 CPNI Order*, 13 FCC Rcd at 8198, para. 198.

[20] 47 CFR § 64.2009(c); *see also 1998 CPNI Order*, 13 FCC Rcd at 8198-99, para. 199.

The Commission's rulemaking and enforcement regarding section 222 have evolved over time to keep pace with emerging threats to consumer privacy.[21]

8. *FCC Data Breach Notification Rule*. Spurred to act by the then-increasing problem of fraud perpetrated through "pretexting," in 2007 the Commission amended its rules to require carriers to notify law enforcement and customers of security breaches involving CPNI.[22] For the purpose of this rule, the Commission defined a "breach" as occurring "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[23] Under this rule, telecommunications carriers must notify the Secret Service and the FBI through a central reporting facility no later than seven business days after a reasonable determination of a breach.[24] With limited exceptions,[25] the rule also prohibits telecommunications carriers from notifying affected customers or disclosing the breach publicly until seven business days following notification to the Secret Service and the FBI.[26] The Commission declined to specify the precise content of the notice that must be provided to customers in the event of a breach of CPNI, leaving telecommunications carriers discretion to tailor the language and method of notification to the circumstances.[27]

9. In 2013, the Commission adopted rules to protect the privacy of customer information relating to all relay services authorized under section 225 of the Act.[28] In that proceeding, the Commission applied CPNI protections to TRS providers, to protect the CPNI of TRS users.[29] The rules

[21] *See generally, e.g.*, *2007 CPNI Order*; *2013 CPNI Declaratory Ruling*.

[22] *2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32.

[23] 47 CFR § 64.2011(e). Note that section 222 of the Act and the Commission's CPNI rules (47 CFR § 64.2001, *et seq*.) related to "access" to customer information make no mention of and do not require that such information be copied, downloaded, exfiltrated, or otherwise acquired. *See generally id.* § 64.2001, *et seq*.; *see also id.* § 64.2010(a) (requiring carriers to "protect against attempts to gain . . . access" to customer information).

[24] *Id.* § 64.2011(b). Additionally, the Commission's rules require carriers to maintain a record of any discovered breaches, notifications to the Secret Service and the FBI regarding those breaches, as well as for a period of at least two years. This record must include, if available, the date that the carrier discovered the breach, the date that the carrier notified the Secret Service and the FBI, a detailed description of the CPNI that was breached, and the circumstances of the breach. *See id.* § 64.2011(d).

[25] Telecommunications carriers can immediately notify a customer or disclose the breach publicly only after consultation with the relevant investigative agency and only if the carrier believed that there was an extraordinarily urgent need to notify a customer or class of customers in order to avoid immediate and irreparable harm. *See id.* § 64.2011(b)(2) (requiring a telecommunications carrier to indicate its desire to notify its customer or class of customers immediately in the notice that it provides to the Secret Service and FBI).

[26] This waiting period for customer notification may be extended by law enforcement if "the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security." *See id.* § 64.2011(b)(3).

[27] *2007 CPNI Order*, 22 FCC Rcd at 6945, para. 32.

[28] *Structure and Practices of the Video Relay Service Program*; *Telecommunications Relay Services and Speech-to-Speech Services for Individuals with Hearing and Speech Disabilities*, CG Docket Nos. 10-51 and 03-123, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 8618, 8680, para. 155 (2013) (*2013 VRS Reform Order*); 47 CFR § 64.5111. In particular, the Commission "establish[ed] customer privacy requirements for TRS pursuant to the specific mandate of section 225(d)(1)(A) to establish 'functional requirements, guidelines, and operations procedures' for TRS," and also found that it had ancillary authority to adopt those rules as well as rules governing point-to-point video services handled over the VRS network. *2013 VRS Reform Order*, 28 FCC Rcd at 8685-87, paras. 170-71.

[29] *2013 VRS Reform Order*, 28 FCC Rcd at 8684, para. 164.

that the Commission adopted were modeled after the CPNI data breach reporting rule applicable to telecommunications services, with minor modifications to account for the unique nature of TRS. [30]

10. As part of a larger proceeding addressing privacy requirements for broadband Internet access service providers (ISPs), in 2016 the Commission revised its breach notification rule and required that those providers (and other telecommunications providers) notify the affected customers, the Commission, the FBI, and the Secret Service of data breaches unless the provider reasonably determined that no harm to customers was reasonably likely to occur.[31] In 2017, however, Congress nullified those 2016 revisions to the Commission's CPNI rules under the Congressional Review Act.[32]

11. *State and Federal Data Breach Notification Laws and Regulations.* The Commission's data breach rule is "not intend[ed] to supersede any statute, regulation, order, or interpretation in any state, except to the extent that such statute regulation, order, or interpretation is inconsistent with [its] provisions,"[33] and the Commission has explicitly rejected requests to preempt all state CPNI obligations, finding instead that states should also be allowed to create rules for protecting CPNI provided that they do not conflict with federal law.[34]

12. Currently, all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have laws requiring covered entities to notify individuals of data breaches.[35] Many state and

[30] *Id.* at 8684, para 165.

[31] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, 31 FCC Rcd 13911, 14019-33, paras. 261-91 (2016) (*2016 Privacy Order*). In 2015, the Commission classified broadband Internet access service as a telecommunications service subject to Title II of the Act, a decision that the D.C. Circuit upheld in *United States Telecom Ass'n v. FCC*. *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5733, para. 306 (2015), *aff'd*, *United States Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016). As a result of classifying broadband Internet access service as a telecommunications service, such services were subject to section 222 of the Act. The rules the Commission adopted in the *2016 Privacy Order* applied to carriers and interconnected VoIP providers in addition to ISPs. *See 2016 Privacy Order*, 31 FCC Rcd at 13925, para. 39, 14033-34, para. 293. In 2017, the Commission reversed the 2015 classification decision so that many Title II obligations, such as section 222, no longer apply to ISPs. *Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2017) (subsequent history omitted).

[32] *See* Joint Resolution, Pub. L. No. 115-22, 131 Stat. 88 (2017) (Resolution of Disapproval) ("*Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,* That Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016)), and such rule shall have no force or effect."); 5 U.S.C. § 801(f) ("Any rule that takes effect and later is made of no force or effect by enactment of a joint resolution under section 802 shall be treated as though such rule had never taken effect."); *id.* § 801(b)(1) ("A rule shall not take effect (or continue), if the Congress enacts a joint resolution of disapproval . . . of the rule."); *see also Protecting the Privacy of Customers of Broadband and Other Telecommunications Services; Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, WC Docket No. 16-106, CC Docket No. 96-115, Order, 32 FCC Rcd 5442 (2017) (*2017 CRA Disapproval Implementation Order*).

[33] 47 CFR § 64.2011(f).

[34] *See 2007 CPNI Order*, 22 FCC Rcd at 6957-58, para. 60 (recognizing that many states have laws relating to the safeguarding of personal information such as CPNI, and to the extent those laws do not create a conflict with federal requirements, carriers are able to comply with both federal and state law); *see also id*. at 6945, para. 31; 47 CFR 64.2011(f).

[35] *See Data Breach Notice* at 5, para. 7 (citing Nat'l Conf. of State Legislatures, *Security Breach Notification Laws* (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

federal data breach frameworks have evolved since the Commission last visited this issue in 2007.[36] Some states, such as California, Virginia, and Colorado, have enacted comprehensive consumer privacy laws in recent years to protect consumers from, among other threats, the ever-growing harms of breaches of personal information.[37] Additionally, several sector-specific breach notification laws exist in the United States, such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the Federal Trade Commission (FTC)-enforced Health Breach Notification Rule, which all have customer notification requirements for breaches of individual data.[38] In July of this year, the Securities and Exchange Commission (SEC) adopted rules requiring public companies to disclose any cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant.[39]

13. *Notice of Proposed Rulemaking*. On December 28, 2022, the Commission adopted a Notice of Proposed Rulemaking (*Data Breach Notice*) seeking comment on several proposed updates to telecommunications carriers' and TRS providers' breach notification duties.[40] In the *Data Breach Notice*, the Commission noted that in the decade and a half since the data breach rule was adopted, breaches of customer information have increased in scale and sophistication, extending far beyond the "pretexting" practices that originally motivated the Commission to act.[41] Additionally, the Commission noted that both Congress and the states have since taken action to protect consumers from the dangers associated with breaches of personal information across sectors.[42] Accordingly, to better protect consumers from the dangers associated with security breaches of customer information and to ensure that our rules keep pace with modern challenges, the Commission proposed to strengthen and update its data breach rules for

[36] *See, e.g.*, American Recovery and Reinvestment Act, Pub. L No. 111-5, 123 Stat. 258, §§ 13400-13402 (2009); Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. Law 111-203, 124 Stat. 1376, §1093 (2010); Cal. Civ. Code §§ 1798.82 (amended 2020); Del. Code § 12B-102 (amended 2017); Wash. Rev. Code § 19.252.01 (amended 2019).

[37] *See Data Breach Notice* at 7, para. 9 (citing Cal. Civ. Code §§ 1798.100.199; State of California Department of Justice, *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa (last visited Jan. 4, 2023); IAPP, *The California Privacy Rights Act*, https://iapp.org/resources/article/the-california-privacy-rights-act-of-2020 (last visited Jan. 4, 2023); Sarah Rippy, *Virginia Passes the Consumer Data Protection Act* (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act; GibsonDunn, *The Colorado Privacy Act: Enactment of Comprehensive U.S. State Consumer Privacy Laws Continues* (July 9, 2021), https://www.gibsondunn.com/the-colorado-privacy-act-enactment-of-comprehensive-u-s-state-consumer-privacy-laws-continues).

[38] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (HIPAA); Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (GLBA); 16 CFR § 318.3. Furthermore, as the *Data Breach Notice* noted, the FTC has also brought actions under section 5(a) of the FTC Act raising allegations that companies acted unfairly by failing to protect consumer data thereby resulting in security breaches, and has published extensive guidance for businesses in the event of a security breach of customer information, including best practices after a data breach has occurred. *Data Breach Notice* at 5, para. 7.

[39] Press Release, SEC, *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (Jul. 26, 2023), https://www.sec.gov/news/press-release/2023-139. The disclosure will generally be due four business days after a registrant determines that an incident is material, but may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. *Id.*

[40] *See generally Data Breach Notice*.

[41] *Id.* at 6, para. 8 (referencing several examples of serious data breaches involving major telecommunications carriers affecting millions of customers).

[42] *Id.* at 6-7, para. 9.

CPNI and TRS to provide greater protections to the public, and sought comment on how best to accomplish this, including on whether our rules should address breaches of other types of sensitive customer information beyond CPNI.[43]

III. DISCUSSION

14. In this Order, we adopt several of the *Data Breach Notice*'s proposals to modernize our data breach requirements.[44] We first expand the scope of our breach notification rules to cover not just CPNI, but all PII. We next adopt the Commission's proposal to expand our definition of "breach" for telecommunications carriers to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier, and such information is not used improperly or further disclosed. We also adopt the Commission's proposal to require carriers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable, but no later than seven business days, after reasonable determination of a breach. We next eliminate the requirement that carriers notify customers of a breach in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. We also eliminate the mandatory waiting period for carriers to notify customers, and instead require carriers to notify customers of breaches of covered data without unreasonable delay after notification to federal agencies, and in no case more than 30 days following reasonable determination of a breach, unless a delay is requested by law enforcement. Finally, to ensure that TRS consumers enjoy the same level of protection under our rules as consumers of telecommunications services, we adopt equivalent requirements for TRS providers.

A. Defining "Breach"

1. Scope of Protected Consumer Information

15. In the *Data Breach Notice*, the Commission recognized that carriers possess proprietary information of customers other than CPNI, which customers have an interest in protecting from public exposure; the notice sought comment on requiring carriers to report breaches of such information.[45] We now conclude that carriers should be obligated to comply with our breach notification rule whenever such information is the subject of a breach, whether or not the information is CPNI.

16. The pervasiveness of data breaches and the frequency of breach notifications have evolved and increased since the Commission first adopted its breach notification rule in 2007. As discussed in the *Data Breach Notice*, our requirement is one of several sector-specific federal breach notification laws in the United States.[46] All state data breach notification requirements explicitly include categories of sensitive personal information within their scope,[47] as do sector-specific federal laws.[48] We

[43] *Id.* at 7-8, 12, 21, paras. 10, 22, 43.

[44] To the extent that this Report and Order does not expressly address a topic that was subject to comment in the *Data Breach Notice*, that issue remains pending.

[45] *Data Breach Notice* at 12, para. 22.

[46] *Id.* at 6-7, para. 9.

[47] *See, e.g.*, La. Rev. Stat. § 3073(4)(a) (defining "personal information" to mean the first name or first initial and last name of an individual in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: (i) social security number; (ii) Driver's license number or state identification card number; (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) Passport number; (v) Biometric data); *see also* Ala. Code § 8-38-2(6); Alaska Stat. § 45.48.090(7); Ariz. Rev. Stat. § 18-551(7), (11); Ark. Code § 4-110-103(7); Cal. Civ. Code § 1798.29(g)-(h); Colo. Rev. Stat. § 6-1-716(1)(d); Conn. Gen. Stat. § 36a-701b(a); D.C. Code § 28-3851(3); Del. Code tit. 6, § 12B-101(7); Fla. Stat. § 501.171(1)(g); Ga. Code § 10-1-911(7); 9 GCA § 48.20(f); Haw. Rev. Stat. § 487N-1; Idaho Stat. § 28-51-104(5); 815 ILCS § 530/5; Ind. Code § 4-1-11-3; Iowa Code § 715C.1(11); Kan. Stat. § 50-7a01(g); KRS § 365.732(1)(c); KRS § 61.931(6); (continued….)

believe that the unauthorized exposure of sensitive personal information that the carrier has received from the customer (i.e., information "of the customer"), or about the customer (i.e., information "relating to" the customer), in connection with the customer relationship (e.g., initiation, provision, or maintenance, of service), such as social security numbers or financial records, is reasonably likely to pose risk of customer harm. Accordingly, any unauthorized disclosure of such information warrants notification to the customer, the Commission, and other law enforcement. Consumers expect that they will be notified of substantial breaches that endanger their privacy, and businesses that handle sensitive personal information should expect to be obligated to report such breaches.[49]

17. We require notification of breaches that involve PII, which is a well-understood concept and thus a readily administrable way of requiring breach notifications in the case of proprietary information.[50] The definition of PII is aptly described in OMB Circular A-130, "Managing Information as a Strategic Resource," as "information that can be used to distinguish or trace an individual's identity,

(Continued from previous page)
Me. Rev. Stat. tit. 10 § 1347(6); Md. Code Com. Law § 14-3501(e); Md. State Govt. Code § 10-1301(c); Mass. Gen. Laws § 93H-1(a); Mich. Comp. Laws § 445.63(q)-(r); Minn. Stat. § 325E.61 Subd. 1(e); Miss. Code § 75-24-29(2)(b); Mo. Rev. Stat. § 407.1500 1. (5)-(6), (9); Mont. Code § 2-6-1501(4); Mont. Code § 30-14-1704(4)(b); Neb. Rev. Stat. § 87-802(5); Nev. Rev. Stat. § 603A.040; N.H. Rev. Stat. § 359-C:19(IV); N.J. Stat § 56:8-161; N.M. Stat. § 57-12C-2(C); N.Y. Gen. Bus. Law § 899-AA(a)-(b); N.C. Gen. Stat § 75-61(10); N.C. Gen. Stat § 14-113.20(b); N.D. Cent. Code § 51-30-01(4); Ohio Rev. Code § 1347.12(A)(6); Ohio Rev. Code § 1349.19(A)(7); Okla. Stat. § 74-3113.1(D)(2); Okla. Stat. § 24-162(6); Oregon Rev. Stat. § 646A.602(12); 73 Pa. Stat. § 2302; 10 L.P.R.A. § 4051(a); R.I. Gen. Laws § 11-49.3-3(a)(8); S.C. Code § 39-1-90(D)(3); S.D. Cod. Laws § 20-40-19(4); Tenn. Code § 47-18-2107(a)(4); Tex. Bus. & Com. Code § 521.002(a)-(b); Utah Code § 13-44-102(4); 9 V.S.A. § 2430(10); Va. Code § 18.2-186.6(A); V.I. Code tit. 14, § 2208(e)-(f); Wash. Rev. Code § 19.255.005(2); W.V. Code § 46A-2A-101(6); Wis. Stat. § 134.98(1)(b); Wyo. Stat. § 40-12-501(a)(vii); Wyo. Stat. § 6-3-901(b).

[48] *See, e.g.*, GLBA Privacy Rule, 16 CFR § 313.3(o) (defining personally identifiable financial information as any information (i) that a consumer provides to the financial institution to obtain a financial product or service; (ii) about a consumer resulting from any transaction involving a financial product or service between the financial institution and a consumer; or (iii) the financial institution otherwise obtains about a consumer in connection with providing a financial product or service to that consumer).

[49] *See, e.g.*, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.*, CG Docket No. 02-278 et al., Declaratory Ruling and Order, 30 FCC Rcd 7961, 8025, para. 132 (2015) (Calls reporting data breaches or conveying remediation information following a breach are "intended to address exigent circumstances in which a quick, timely communication with a consumer could prevent considerable consumer harms from occurring or, in the case of the remediation calls, could help quickly mitigate the extent of harm that will occur."); *TerraCom NAL*, 29 FCC Rcd at 13340-41, para. 43 ("We expect carriers to act in an abundance of caution . . . in their practices with respect to notifying consumers of security breaches.").

[50] We reject claims that we did not provide sufficient notice to define the scope of protected consumer information in this manner. *See, e.g.*, Letter from Avonne Bell, Director, Connected Life, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 10-11 (filed Dec. 6, 2023) (CTIA Dec. 6, 2023 *Ex Parte*); T-Mobile Dec. 6, 2023 *Ex Parte* at 4. In the *Data Breach Notice* we sought comment on "requir[ing] telecommunications carriers to report breaches of proprietary information other than CPNI under Section 222(a)," in which case commenters were asked to address "how broadly or narrowly [we should] define that category of information." *Data Breach Notice* at 12, para. 22. This provided notice that the Commission could define the scope of protected information to encompass all or any subset of the universe of proprietary information under section 222(a). And as we explain below, we conclude that the scope of customer information encompassed by section 222(a) is best interpreted to include PII, and define the scope of our breach notification rules to include PII subject to the additional limitations that we adopt below. *See infra* paras. 18, 70. We therefore conclude that there was sufficient notice for the approach we adopt.

either alone or when combined with other information that is linked or linkable to a specific individual."[51] CPNI is a subset of PII.[52]

18. For the purposes of our breach notification rules, we further define the scope of covered PII as (1) first name or first initial, and last name, in combination with any government-issued identification numbers or information issued on a government document used to verify the identity of a specific individual,[53] or other unique identification number used for authentication purposes;[54] (2) user name or e-mail address, in combination with a password or security question and answer, or any other authentication method or information necessary to permit access to an account;[55] or (3) unique biometric, genetic, or medical data.[56] Moreover, dissociated data that, if linked, would constitute PII is to be

[51] Off. of Mgmt. & Budget, *Managing Information as a Strategic Resource*, OMB Circular No. A-130 § 10(57) (2016) (OMB Circular No. A-130), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

[52] As discussed below, this approach of holding carriers responsible for reporting breaches of PII is supported independently and alternatively by construing the phrase "proprietary information of . . . customers" in section 222(a) as covering all information defined as PII, and by recognizing that section 201(b)'s just-and-reasonable-practices obligation requires protection of PII. *See infra* Section III.E.1-2; 47 U.S.C. § 222(a).

[53] Including, but not limited to, Social Security Number, driver's license number or state identification number, Taxpayer Identification Number, passport number, military identification number, Tribal identification card, or any other Federal or state government-issued identification card. *See, e.g.*, Ala. Code § 8-38-2(6)(a)(1)-(2); Alaska Stat. § 45.48.090(7)(B)(i); Ariz. Rev. Stat. § 18-551(11)(a); Ark. Code § 4-110-103(7)(A); Cal. Civ. Code § 1798.82(h)(1)(A); Colo. Rev. Stat. § 6-1-716(1)(g)(I)(A); Conn. Gen. Stat. § 36a-701b(a)(2)(A)(i); Del. Code tit. 6 § 12B-101(7)(a)(1); D.C. Code § 28-3851(3)(A)(i)(I); Fla. Stat. § 501.171(1)(g)(1)(a)(I); Ga. Code § 10-1-911(6)(A); 9 GCA § 48.20(f)(1); Haw. Rev. Stat. § 487N-1.

[54] Including, but not limited to, a financial institution account number, student identification number, or medical identification number. *See, e.g.*, Colo. Rev. Stat. § 6-1-716(1)(g)(I)(A); Wash. Rev. Code § 19.255.005(2)(a)(i)(F); Okla. Stat. tit. 24 § 162(6)(c); Oregon Rev. Stat. § 646A.602(12)(a)(A)(iv); 73 Pa. Stat. § 2302; 10 L.P.R.A. § 4051(a)(3); R.I. Gen. Laws § 11-49.3-3(a)(8)(iii); S.C. Code § 39-1-90(D)(3)(c); S.D. Cod. Laws § 22-40-19(4)(c); S.D. Cod. Laws § 22-40-19(5)(b); Tenn. Code § 47-18-2107(a)(4)(A)(iii); Tex. Bus. & Com. Code § 521.002(a)(2)(A)(iii); V.I. Code tit. 14, § 2209(e)(3); Utah Code § 13-44-102(4)(a)(ii); 9 V.S.A. § 2430(9)(A)(iii); Va. Code § 18.2-186.6(A); Wash. Rev. Code § 19.255.005(2)(a)(i)(C); W.V. Code § 46A-2A-101(6)(C); Wis. Stat. § 134.98(1)(b)(3); Wyo. Stat. § 40-12-501(a)(vii) (citing Wyo. Stat. § 6-3-901(b)(v)).

[55] Including, but not limited to, Personal Identification Numbers, private keys that are unique to an individual and are used to authenticate or sign an electronic record; unique electronic identifiers or routing codes, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or shared secrets or security tokens that are known to be used for data-based authentication. *See, e.g.*, Ala. Code § 8-38-2(6)(a)(6); Ariz. Rev. Stat. § 18-551(7)(a)(ii), (11)(c); Cal. Civ. Code § 1798.82(h)(2); Colo. Rev. Stat. § 6-1-716(1)(g)(I)(A); Conn. Gen. Stat. § 36a-701b(a)(2)(A)(x); D.C. Code § 28-3851(3)(A)(ii); Del. Code tit. 6 § 12B-101(7)(a)(5); Fla. Stat. § 501.171(1)(g)(1)(b); 815 ILCS § 530/5; Md. Code, Com. § 14-3501(e)(1)(ii); Neb. Rev. Stat. § 87-802(5)(b); Nev. Rev. Stat. § 603A.040(1)(e); N.J. Stat. § 56:8-161; N.Y. Gen. Bus. Law § 899-aa(1)(b)(ii); N.C. Gen. Stat § 14-113.20(b)(8); Oregon Rev. Stat. § 646A.602(12)(a)(B); 10 L.P.R.A. § 4051(a)(4); R.I. Gen. Laws § 11-49.3-3(a)(8)(v); S.D. Cod. Laws § 22-40-19(5); Wash. Rev. Code § 19.255.005(2)(a)(i), (ii); Wyo. Stat. § 40-12-501(a)(vii) (citing Wyo. Stat. § 6-3-901(b)(ix)).

[56] Including, but not limited to, fingerprints, faceprint, a retinal or iris scan, hand geometry, voiceprint analysis, or other unique biometric data generated from a measurement or analysis of human body characteristics to authenticate or ascertain an individual's identity; genetic data such as deoxyribonucleic acid data; and medical records, or other information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. *See, e.g.*, Ariz. Rev. Stat. § 18-551(11)(i); Ark. Code § 4-110-103(7)(E); Cal. Civ. Code § 1798.82(h)(1)(F); Colo. Rev. Stat. § 6-1-716(1)(g)(I)(A); Conn. Gen. Stat. § 36a-701b(a)(2)(A)(ix); D.C. Code § 28-3851(3)(A)(i)(VI); Del. Code tit. 6 § 12B-101(7)(a)(8); 815 ILCS § 530/5; Iowa Code § 715C.1(11)(a)(5); La. Rev. Stat. § 51:3073(4)(a)(v); Md. Code, Com. § 14-3501(e)(1)(i)(6); Neb. Rev. Stat. § 87-802(5)(a)(v); N.M. Stat. § 57-12C-2(C)(1)(e); N.Y. Gen. Bus. Law § 899-aa(1)(b)(i)(5); N.C. Gen. Stat § 14-113.20(b)(11); Oregon Rev. Stat. § 646A.602(12)(a)(A)(v); Tex. Bus. & Com. Code § 521.002(a)(1)(C); 9 V.S.A. § (continued….)

considered PII if the means to link the dissociated data were accessed in connection with access to the dissociated data, and any one of the discrete data elements listed above or any combination of the discrete data elements listed above is PII if the data element or combination of data elements would enable a person to commit identity theft or fraud against the individual to whom the data element or elements pertain.[57]

19. Our approach brings our definition of covered data in line with the approaches taken at the state level, and responds to concerns raised in the record by certain parties regarding harmonization with existing breach notification regimes.[58] In order to further harmonize our approach with analogous state law, we also adopt an exception from our definition of PII for publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.[59] Notwithstanding these limitations, we will monitor the data security landscape and will not hesitate to revisit and revise the list of data elements in a future rulemaking as necessary to ensure that carriers adequately protect sensitive customer data.

20. Without an FCC rule requiring breach notifications for the above categories of PII, there would be no requirement in federal law that telecommunications carriers report non-CPNI breaches to their customers. CTIA's objection that doing so would "[c]reat[e] a system of dual jurisdiction between the FCC and the FTC"[60] is unpersuasive. CTIA asserts that "[c]ustomers do not expect different privacy protections for the same data depending on which entity holds the data or the kind of product or service that is being marketed" but concedes the FTC's lack of authority in the common carrier context.[61] By the statutory design of the Communications Act and the FTC Act, Congress assigned differing areas of responsibility to the FCC and FTC, and CTIA identifies no grounds for the Commission to ignore its responsibilities with respect to common carriers. By ensuring that the same data breach notification requirements also apply to interconnected VoIP and TRS providers, we advance the interest of ensuring that consumers can have the same expectations regarding services that they view as similar. The approach we adopt today therefore not only reflects the practical expectations of consumers but also honors the intention of Congress.[62] Despite NCTA's suggestion that "there is no other 'proprietary information' between a provider and its customer that is not CPNI but is covered by Section 222,"[63] the Commission has investigated several instances of breaches involving sensitive personal information about

(Continued from previous page)
2430(9)(A)(v); Wash. Rev. Code § 19.255.005(2)(a)(i)(I); Wis. Stat. § 134.98(1)(b)(5); Wyo. Stat. § 40-12-501(a)(vii) (citing Wyo. Stat. § 6-3-901(b)(xiii)).

[57] *See, e.g.*, D.C. Code § 28-3851(3)(A)(i)(VII); N.J. Stat. § 56:8-161; Oregon Rev. Stat. § 646A.602(12)(a)(C)(ii); Wash. Rev. Code § 19.255.005(2)(a)(iii)(B).

[58] *See* Letter from Steven Morris, Vice President & Deputy General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 2-3 (filed Dec. 5, 2023) (NCTA Dec. 5, 2023 *Ex Parte*) at 2-3; CTIA Dec. 6, 2023 *Ex Parte* at 11-12; USTelecom Dec. 6, 2023 *Ex Parte* at 1-2.

[59] *See, e.g.*, Ala. Code § 8-38-2(6)(b)(1); Ariz. Rev. Stat. § 18-551(7)(b); Cal. Civ. Code § 1798.82(i)(1); Colo. Rev. Stat. § 6-1-716(1)(g)(II); Conn. Gen. Stat. § 36a-701b(2)(A)(x); Del. Code tit. 6 § 12B-101(7)(b); Ga. Code § 10-1-911(6)(E); ILCS § 530/5; La. Rev. Stat. § 51:3073(4)(b); Me. Rev. Stat. tit. 10 § 1347(6); Minn. Stat. § 325E.61 Subd. 1(f)).

[60] CTIA Reply at 7.

[61] *Id.* at 7; *see also* 15 U.S.C. § 45(a)(2).

[62] For example, as discussed in more detail below, Congress ratified the Commission's 2007 decision to extend section 222-based privacy protections for telecommunications service customers to the customers of interconnected VoIP providers. *See infra* Section III.E.3. And ensuring equivalent protections for TRS subscribers advances Congress' directive to endeavor to ensure functionally equivalent service. *See infra* Section III.E.4.

[63] NCTA Comments at 13.

customers held by telecommunications carriers that was not or may not have been CPNI.[64] The Commission has also in the past concluded that names, addresses, and telephone numbers are not CPNI, even when a customer has elected not to have them disclosed publicly, and that such information therefore would not be subject to the CPNI-specific restrictions on use in section 222(c).[65] We find that such information can be sensitive and warrants protection, including a requirement that the Commission, law enforcement, and customers be notified about breaches. Indeed, because consumers expect to be notified of substantial breaches that endanger their privacy, it better protects customers that breach notifications not turn on whether a particular breached element is or is not CPNI.

2. Inadvertent Access, Use, or Disclosure of Covered Data

21. Consistent with the *Data Breach Notice*'s proposal, we expand the Commission's definition of "breach" to include inadvertent access, use, or disclosure of covered data.[66] Specifically, we define "breach" as any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed covered data.[67] While the practice of pretexting that spurred the Commission to act in 2007 necessarily involves an intent to gain access to customer information, the record before us here amply demonstrates that the inadvertent exposure of customer information can result in the loss and misuse of sensitive information by scammers and phishers, and trigger a need to inform the affected individuals so that they can take appropriate steps to protect themselves and their information.[68] We agree with the wide range of commenters that recognize that any exposure of customer

[64] *See, e.g.*, *TerraCom NAL*, 29 FCC Rcd at 13330-32, paras. 13-20.

[65] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Information*, Order, 13 FCC Rcd 12390, 12395-96, paras. 8-9 (WCB 1998) (*1998 CPNI Clarification Order*) (finding that names, addresses, and telephone numbers are not CPNI and therefore that carriers may use such information for marketing purposes).

[66] *See Data Breach Notice* at 8-9, paras. 12, 14.

[67] *See infra* Appx. A.

[68] *See, e.g.*, EPIC Comments at 2; WISPA Comments at 2; NRECA Reply at 2; *cf., e.g.*, Shawn Snow, *Major Data Breach at Marine Forces Reserve Impacts Thousands*, Marine Corps Times (Feb. 28, 2018), https://www.marinecorpstimes.com/news/your-marine-corps/2018/02/28/major-data-breach-at-marine-forces-reserve-impacts-thousands (describing the accidental disclosure of highly sensitive data of more than 21,000 service members, including truncated social security numbers, electronic funds transfer and bank routing numbers, truncated credit card information, mailing and residential addresses, and emergency contact information, caused by the transmission of an unencrypted email with an attachment to the wrong distribution list); Jan Murphy, *Data Breach Put 360,000 Pa. Teachers, Education Department Staffers' Personal Information at Risk*, PennLive (Mar. 23, 2018), https://www.pennlive.com/politics/2018/03/data_breach_put_360000_pa_teac.html (reporting that human error led to the accidental exposure of highly sensitive information of approximately 360,000 current and retired teachers in Pennsylvania, including users' social security numbers); *Melbourne Student Health Records Posted Online in 'Appalling' Privacy Breach: Health and Medication Data Posted in Error on Strathmore Secondary College Intranet*, Guardian (Aug. 21, 2018), https://www.theguardian.com/australia-news/2018/aug/22/melbourne-student-health-records-posted-online-in-appalling-privacy-breach (reporting that in August 2018, the personal records of more than 300 students at Strathmore secondary college in Melbourne, Australia were accidentally published to the school's intranet service, resulting in the inadvertent disclosure of data relating to medical and mental health conditions, medications, and learning and behavioral difficulties for hundreds of high school students); Volodymyr "Bob" Diachenko, *Veeam Inadvertently Exposed Marketing Database with Hundreds of Millions of Records*, LinkedIn (Sept. 11, 2018), https://www.linkedin.com/pulse/veeam-inadvertently-exposed-marketing-info-hundreds-its-bob-diachenko (reporting on an exposed database that had been accidentally made available on the Internet by Veeam, a company that develops backup, disaster recovery, and intelligent data management software for virtual, physical, and multi-cloud infrastructures, which contained more than 200 gigabytes of customer records, including names, several hundred million email addresses, and IP addresses).

data can risk harming consumers, regardless of whether the exposure was intentional.[69] As the Accessibility Advocacy and Research Organizations (AARO) argue, "[t]he Commission must adapt to an ever changing technological environment, which implicates all kinds of privacy concerns, and adopt measures that can effectively counter increasingly complex and evolving breaches."[70] In order to address these risks, carriers not only must reasonably protect covered information as required by the Act and our rules, but also must inform affected individuals so that they can take appropriate steps to protect themselves and their information where breaches occur.[71] In addition, notification of both intentional and unintentional breaches to the Commission and other federal law enforcement will aid investigations and help prevent new breaches or further harm to consumers.[72] We expect that our broadening of "breach" to include inadvertent exposure will encourage telecommunications carriers to adopt stronger data security practices, and will help federal agencies identify and address systemic network vulnerabilities.[73]

22. The record supports the Commission's observation in the *Data Breach Notice* that breaches have become more prevalent and more severe in recent years.[74] In 2021, the Identity Theft Resource Center "estimated a record-breaking 1,862 data breaches," and a survey from IBM has exposed "a recent decline in response capabilities" due to "informal or ad hoc" data security plans.[75] This rising tide of data breaches has affected the telecommunications sector as well. As the Electronic Privacy Information Center (EPIC) points out, the proprietary information of subscribers of each of the three largest carriers "has been breached at least once within the last five years."[76] Indeed, in February 2020, the Commission proposed more than $200 million in fines against AT&T, Sprint, T-Mobile, and Verizon, for apparently failing to adequately protect consumer location data.[77] In each case, the Commission found that the carriers' apparently lacked adequate oversight over third-party location aggregators' use of their phone subscribers' location data, leading to the disclosure of their respective customers' location information, without consent, to third parties who were not authorized to receive it.[78]

---

[69] *See, e.g.*, ACA Connects Comments at 4 ("[D]isclosures of CPNI can harm consumers whether or not intentional . . . ."); EPIC Comments at 2-3; NCTA Comments at 4; EPIC et al. Reply at 3-4; JFL Reply at 14 ("Potential harms exist whenever a data breach occurs, whether intentional or inadvertent."); *see also Data Breach Notice* at 8, para. 12 n.47.

[70] AARO Reply at 6.

[71] *Data Breach Notice* at 8, para. 12; EPIC Comments at 2.

[72] *Data Breach Notice* at 8, para. 12; *see also* EPIC Comments at 3 (agreeing "with the Commission's analysis that requirements to notify [for] accidental breaches will encourage carriers to adopt stronger data security practices and help the Commission identify and address systemic network vulnerabilities").

[73] *Data Breach Notice* at 8, para. 12; EPIC Comments at 3; NRECA Reply at 3; Letter from David Smith, Assistant Director, Office of Investigations, U.S. Secret Service, to Adam Copeland, Deputy Bureau Chief, FCC, WC Docket No. 22-21, at 1-2 (filed Nov. 7, 2023) (USSS Letter).

[74] *Data Breach Notice* at 1-2, para. 1; *see also* Confidentiality Coalition Comments at 2 (reporting a 118% increase from 2020 to 2021 in unauthorized access incidents, and a 44% increase in ransomware attacks impacting publicly traded companies); Lincoln Network Comments at 3.

[75] EPIC Comments at 3 (citing *Record Number of Data Breaches in 2021*, IAPP Daily Dashboard (Jan. 25, 2022), https://iapp.org/news/a/record-number-of-data-breaches-in-2021 (citing to ITRC report)); IBM Security, *Cyber Resilient Organization Study* at 8 (2020), https://www.ibm.com/account/reg/us-en/signup?formid=urx-45839.

[76] EPIC Comments at 3-4.

[77] Press Release, FCC, FCC Proposes Over $200 Million in Fines Against Four Largest Wireless Carriers for Apparently Failing to Adequately Protect Consumer Location Data (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations.

[78] *See, e.g.*, *AT&T, Inc.*, File No.: EB-TCD-18-00027704, Notice of Apparently Liability for Forfeiture and Admonishment, 35 FCC Rcd 1743, 1744, para. 3 (2020).

23. Given these worrying trends, we agree with EPIC that our expansion of "breach" to include inadvertent exposures is a necessary first step to galvanize carriers to strengthen their data security policies and oversight of customer data. In particular, our broadening of the breach definition will better enable the marketplace to respond to the relative strengths of particular carriers' practices and enhance the Commission's ability to identify where additional regulatory oversight might be needed.[79] Removing the intent limitation in our breach reporting rule will reduce ambiguity regarding whether reporting a breach is necessary, and therefore decrease the risk of underreporting.[80] Finally, our expansion of "breach" to include inadvertent access, use, or disclosure of customer information brings our rules in line with the overwhelming majority of state and federal breach notification laws and regulations that lack such an intent limitation, ensuring that consumers nationwide—along with the Commission and other relevant federal authorities—likewise receive critical breach notifications in a timely manner.[81]

24. Notwithstanding these benefits, we acknowledge concerns expressed by carriers that our expansion of the "breach" definition to include inadvertent disclosures, on its own, could lead to "notice fatigue" for consumers,[82] deplete Commission and law enforcement resources,[83] or increase the burden of reporting obligations.[84] In response to these concerns, as discussed below, we exempt from our expanded

[79] EPIC Comments at 3.

[80] *Id.* at 2-3.

[81] The data breach laws in 49 states and four U.S. Territories have no intent limitation, and neither do the breach reporting requirements for federal agencies, established by the Office of Management and Budget (OMB), or the notification regulations for the Department of Health and Human Services and Federal Trade Commission. *See, e.g.*, Ala. Code § 8-38-2(1); Alaska Stat. § 45.48.090; Ariz. Rev. Stat. § 18-551(1)(a); Ark. Code § 4-110-103(1)(A); Cal. Civ. Code § 1798.82(g); Colo. Rev. Stat. § 6-1-716(1)(h); Conn. Gen. Stat. § 36a-701b(a); Del. Code tit. 6 § 12B-101(1)(a); D.C. Code § 28-3851(1); Fla. Stat. § 501.171(1)(a); Ga. Code § 10-1-911(1); 9 GCA § 48.20(a); Haw. Rev. Stat. § 487N-1; 815 ILCS § 530/5; Ind. Code § 24-4.9-2-2; Iowa Code § 715C.1(1); Kan. Stat. § 50-7a01(h); KRS § 365.732(1)(a); La. Rev. Stat. § 51:3073(2); Me. Rev. Stat. tit. 10 § 1347(1); Md. Code Com. Law § 14-3504(a)(1); Mass. Gen. Laws § 93H-1(a); Mich. Comp. Laws § 445.63(b); Minn. Stat. § 325E.61 Subd. 1(d); Miss. Code § 75-24-29(2)(a); Mo. Rev. Stat. § 407.1500(1)(1); Mont. Code § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. § 603A.020; N.H. Rev. Stat. § 359-C:19(V); N.J. Stat. § 56:8-161; N.M. Stat. § 57-12C-2(D); N.Y. Gen. Bus. Law § 899-aa(1)(c); N.C. Gen. Stat § 75-61(14); N.D. Cent. Code § 51-30-01(1); Ohio Rev. Code § 1349.19(A)(1)(a); Ohio Rev. Code § 1354.01(C); Okla. Stat. tit. 24 § 162(1); Oregon Rev. Stat. § 646A.602(1); 73 Pa. Stat. § 2302; 10 L.P.R.A. § 4051(c); R.I. Gen. Laws § 11-49.3-3(a)(1); S.C. Code § 39-1-90(D)(1); S.D. Cod. Laws § 22-40-19(1); Tenn. Code § 47-18-2107(a)(1)(A); Tex. Bus. & Com. Code § 521.053(a); Utah Code § 13-44-102(1)(a); 9 V.S.A. § 2430(13)(A); Va. Code § 18.2-186.6(A); V.I. Code tit. 14, § 2208(d); Wash. Rev. Code § 19.255.005(1); W.V. Code § 46A-2A-101(1); Wis. Stat. § 134.98(2)(a)-(b); Wyo. Stat. § 40-12-501(a)(i); *Preparing for and Responding to a Breach of Personally Identifiable Information*, Office of Management and Budget, M-17-12, Memorandum for Heads of Executive Departments and Agencies at 9 (Jan. 3, 2017) (OMB M-17-12); 45 CFR § 164.402; 16 CFR § 318.2(a).

[82] *See, e.g.*, Blooston Rural Carriers Comments at 2; CCA Comments at 4; CrowdStrike Comments at 2; CTIA Comments at 26; Verizon Comments at 1-2, 8; WISPA Comments at 3; NRECA Reply at 3; Southern Linc Reply at 2.

[83] *See, e.g.*, Blooston Rural Carriers Comments at 2; CTIA Comments at 26; NTCA Comments at 4; WISPA Comments at 3; WTA Comments at 7; NRECA Reply at 4.

[84] *See, e.g.*, NTCA Comments at 4; Staurulakis Comments at 2-3; WISPA Comments at 3; WISPA Reply at 2. We are unpersuaded by the arguments of Lincoln Network, which goes even further and contends that data breach reporting requirements would implicate the major questions doctrine. Lincoln Network Comments at 7-8 (arguing that expanding notification requirements to include inadvertent breaches would greatly increase costs for carriers, implicating the major questions doctrine). Lincoln Networks focuses solely on the alleged economic impact of the requirement to the exclusion of other considerations, and even then provides no meaningful sense of the likely magnitude of such effects—citing total estimated economic costs of breaches and asserting in a conclusory manner that "it is reasonable to conclude that at least some of the cost per breach is assignable to notification," without quantifying the cost associated with such notifications, let alone any portion attributable specifically to FCC breach

(continued….)

definition of "breach" a good-faith acquisition of customer data by an employee or agent of a carrier where such information is not used improperly or further disclosed.[85] We also adopt a "harm-based notification trigger," such that notification of a breach to consumers is not required in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed.[86] As discussed below, we also find that our adoption of a minimum threshold for the number of customers affected to trigger our requirement to notify the Commission and other federal law enforcement regarding breaches where there is no reasonable likelihood of harm will further reduce carriers' reporting burdens, and make more efficient use of agencies' resources.[87] Although carriers' obligation to protect covered information under section 222 of the Act and our implementing rules is not limited just to scenarios where there is actual evidence of consumer harms, these common-sense limitations on our disclosure requirements are well-supported by the record,[88] and are consistent with most state and federal data breach notification regimes.[89] Taken together, we find that these carve-outs will mitigate any legitimate concerns expressed by commenters in the record regarding the potential for consumer notice fatigue and undue burdens on federal agencies and carriers by triggering the requirements in situations where we find disclosures most strongly justified.[90]

25. In the *Data Breach Notice*, the Commission also sought comment on whether it should "expand the definition of a breach to include situations where a telecommunications carrier or a third party discovers conduct that could have reasonably led to exposure of customer CPNI, even if it has not yet determined if such exposure occurred."[91] Commenters generally oppose such an expansion,[92] arguing

(Continued from previous page)
notification rules. *Id.* at 8. We thus are unpersuaded that the major questions doctrine is implicated here. In any case, we explain below why these rules fall comfortably within the Commission's statutory authority. *See infra* Section III.E.

[85] *See infra* Section III.A.3 (discussing good-faith exception).

[86] *See infra* Section III.C.1 (discussing harm-based customer notification trigger).

[87] *See infra* Section III.B.2 (discussing threshold trigger); *see, e.g.*, NRECA Reply at 4 (advocating for a threshold trigger for notifications to the Commission or federal law enforcement).

[88] *See, e.g.*, ACA Connects Comments at 4 n.8 (arguing in favor of a good-faith exception); Blooston Rural Carriers Comments at 2; CCA Comments at 4-5; CrowdStrike Comments at 3; CTIA Comments at 27; NCTA Comments at 2, 5; NTCA Comments at 5; Verizon Comments at 9-10; WISPA Comments at 4; NRECA Reply at 4.

[89] *Data Breach Notice* at 9, para. 14 n.50 (listing state notification laws that contain a good-faith exception); *id.* at 10, para. 16 n.53 (listing a selection of state notification laws that contain a harm-based notification trigger); *see also, e.g.*, Ala. Code § 8-38-5(a) (including a harm-based notification trigger); Del. Code tit. 6 § 12B-102(a) (same); Ind. Code § 24-4.9-3-1(a) (same); La. Rev. Stat. § 51:3074(I) (same); Mass. Gen. Laws § 93H-3(b) (same); Mich. Comp. Laws § 445.72(1) (same); Miss. Code § 75-24-29(3) (same); Mo. Rev. Stat. § 407.1500(2)(5) (same); N.Y. Gen. Bus. Law § 899-aa(2)(a) (same); Ohio Rev. Code § 1349.19(B)(1)(a) (same); Okla. Stat. tit. 24 § 163(A) (same); R.I. Gen. Laws § 11-49.3-4(a)(1) (same); S.C. Code § 39-1-90(A) (same); S.D. Cod. Laws § 22-40-20 (same); Utah Code § 13-44-202(1)(b) (same); Va. Code Ann. § 18.2-186.6(B) (same); Wash. Rev. Code § 19.255.010(1) (same); W.V. Code § 46A-2A-102(a) (same); Wis. Stat. § 134.98(2)(cm)(1) (same); Wyo. Stat. § 40-12-502(a) (same).

[90] *See* NCTA Comments at 2 ("If the Commission adopts a reasonable and objective harm-based trigger, NCTA further supports the Commission's proposal to include inadvertent access in the definition of 'breach.'"); *cf.* Sorenson Communications LLC Comments at 2 (Sorenson Comments).

[91] *Data Breach Notice* at 10, para. 14.

[92] ACA Connects Comments at 4-5 n.10; USTelecom Comments at 5-6; WISPA Comments at 4; CTIA Comments at 27; Verizon Comments at 9-10; WTA Reply at 2 (contending that "conduct or security weaknesses that theoretically or potentially could have led to exposure of CPNI (but where there is no evidence that they actually did) are matters for carrier corrective actions and employee training . . .").

that it could result in over-notification to customers and to government entities,[93] impeding carriers' and the government's investigation of actual breaches,[94] and needlessly frightening consumers.[95] While we believe that notification of situations in which customer data are put at risk has value,[96] no commenter in the record provides evidence in support of such an approach. We nevertheless expect that in such situations, carriers will work reasonably and efficiently to confirm whether or not actual exposure has occurred. While we decline at this time to amend the definition of breach to include situations where a carrier or third party has not yet determined if an exposure of covered data has occurred, we also note that we do not prohibit carriers from providing notice in such situations to their customers if, for example, they determine that doing so is appropriate under the circumstances.[97] We also will continue to monitor how such situations impact customers, and reserve the ability to expand the breach definition to cover such situations in the future, should we find such an expansion is warranted.

3. Good-Faith Exception

26. We exclude from the definition of "breach" a good-faith acquisition of covered data by an employee or agent of a carrier where such information is not used improperly or further disclosed.[98] As noted above and in the *Data Breach Notice*,[99] the vast majority of state statutes include a similar exception from the definition of "breach,"[100] and commenters overwhelmingly agree that such an

[93] *See, e.g.*, CTIA Comments at 27; USTelecom Comments at 5-6.

[94] WISPA Comments at 4.

[95] Verizon Comments at 10; WISPA Comments at 4.

[96] *See* Verizon, *Verizon Responds to Report: Confirms No Loss or Theft of Customer Information* (July 12, 2017), https://www.verizon.com/about/news/verizon-responds-report-confirms-no-loss-or-theft-customer-information (notifying the public that an employee of one of Verizon's vendors had put information in cloud storage with settings that could have allowed it to be exposed to the public even though it did not ultimately result in "a loss or theft of Verizon or Verizon customer information"); *cf.* OMB M-17-12, at 14 (requiring reporting of "suspected" breaches to prevent a delay that would undermine an "agency's ability to apply preventative and remedial measures to protect the PII or reduce the risk of harm to potentially affected individuals").

[97] While we have not expanded the definition of data breach to include situations where customer data is put at risk but not exposed, we note that the threshold for reporting a breach is separate from the obligation to "protect the confidentiality of proprietary information" and to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." 47 U.S.C. § 222(a); 47 CFR § 64.2010(a). Not only may a breach that does not meet the reporting threshold still reflect a violation of section 222 of the Act or an unreasonable practice in violation of 64.2010(a) of the rules, but a carrier can violate section 222 of the Act or section 64.2010(a) of the rules even in the absence of any breach.

[98] *Data Breach Notice* at 9, para. 14. In the *Data Breach Notice*, we used the term "exemption" instead of "exception" when asking commenters whether we should exclude from the definition of "breach" a good-faith acquisition of covered data. *See id.* at 10, para. 14. For the purpose of clarity, we instead use the word "exception" here to describe this exclusion. While we make this exception to our definition of "breach," we nevertheless expect carriers to "take reasonable measures" in such scenarios to protect such customer information from improper use or further disclosure, which may, for example, involve requiring that such an employee or agent destroy the data upon realizing that the data was disclosed without, or in excess of, authorization. *Cf.* 47 CFR § 64.2010(a) (requiring telecommunications carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI).

[99] *Data Breach Notice* at 9, para. 14.

[100] *See, e.g.*, Ala. Code § 8-38-2(1); Alaska Stat. § 45.48.050; Ariz. Rev. Stat. § 18-551(1)(b); Ark. Code § 4-110-103(1)(B); Cal. Civ. Code § 1798.82(g); Colo. Rev. Stat. § 6-1-716(1)(h); Del. Code tit. 6 § 12B-101(1)(a); D.C. Code § 28-3851(1); Fla. Stat. § 501.171(1)(a); Ga. Code § 10-1-911(1); 9 GCA § 48.20(a); Haw. Rev. Stat. § 487N-1; Idaho Stat. § 28-51-104(2); 815 ILCS § 530/5; Ind. Code § 4-1-11-2(b)(1); Iowa Code § 715C.1(1); Kan. Stat. § 50-7a01(h); KRS § 365.732(1)(a); La. Rev. Stat. § 51:3073(2); Me. Rev. Stat. tit. 10 § 1347(1); Md. Code Com. Law § 14-3504(a)(2); Mass. Gen. Laws § 93H-1(a); Mich. Comp. Laws § 445.63(b); Minn. Stat. § 325E.61 Subd.

(continued….)

exception is appropriate.[101] As Blooston Rural Carriers argues, a good-faith exception will prevent carriers from "unnecessarily confus[ing] and alarm[ing] consumers" in such low-risk situations.[102] We also agree with National Rural Electric Cooperative Association (NRECA) that, without this exception, "more serious data breaches [will potentially] become lost in the 'noise' of multiple notifications."[103] We therefore find that our good-faith exception will help avoid excessive notifications to consumers, and reduce reporting burdens on carriers.[104]

27. We disagree with EPIC that our adoption of a good-faith exception would "weaken privacy and data security protections for consumers."[105] In support of these claims, EPIC cites instances in which employees, "either through bribery or inadequate training, were illegally disclosing consumer information to pretexters claiming to have authorization to access subscriber information."[106] We do not find that these situations justify taking a different approach; indeed, the exception we adopt today would not apply in the scenarios outlined by EPIC. First, our good-faith exception relieves carriers from reporting obligations only where customer information is not used improperly or further disclosed, and in EPIC's example, the information was, intentionally or not, further disclosed to a pretexter. Second, in circumstances where an employee improperly discloses consumer information due to bribery, the employee disclosing the information is, by definition, not acting in "good faith," and therefore such an incident would still be considered a breach under our rules.

B. Notifying the Commission and Other Federal Law Enforcement of Data Breaches

1. Requiring Notification to the Commission

28. As proposed in the *Data Breach Notice*,[107] we require telecommunications carriers to notify the Commission of a breach in addition to notification to the Secret Service and FBI.[108] The

(Continued from previous page)
1(d); Mo. Rev. Stat. § 407.1500(1)(1); Mont. Code § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. § 603A.020; N.H. Rev. Stat. § 359-C:19(V); N.J. Stat. § 56:8-161; N.M. Stat. § 57-12C-2(D); N.Y. Gen. Bus. Law § 899-aa(1)(c); N.C. Gen. Stat. § 75-61(14); N.D. Cent. Code § 51-30-01(1); Ohio Rev. Code § 1349.19(A)(1)(b)(i); Ohio Rev. Code § 1354.01(C)(1); Okla. Stat. § 24-162(1); Oregon Rev. Stat. § 646A.602(1); 73 Pa. Stat. § 2302; R.I. Gen. Laws § 11-49.3-3(a)(1); S.C. Code § 39-1-90(D)(1); S.D. Cod. Laws § 20-40-19(1); Tenn. Code § 47-18-2107(a)(1)(B); Tex. Bus. & Com. Code § 521.053(a); Utah Code § 13-44-102(1)(b); 9 V.S.A. § 2430(13)(B); Va. Code § 18.2-186.6(A); V.I. Code tit. 14, § 2209(d); Wash. Rev. Code § 19.255.005(1); W.V. Code § 46A-2A-101(1); Wis. Stat. § 134.98(2)(cm)(2); Wyo. Stat. § 40-12-501(a)(i); *see also* CCA Comments at 5; NTCA Comments at 5; Verizon Comments at 9.

[101] *See, e.g.*, ACA Connects Comments at 4 n.8; Blooston Rural Carriers Comments at 2; CCA Comments at 5; CTIA Comments at 27; NCTA Comments at 2; NRECA Reply at 4; NTCA Comments at 5; Verizon Comments at 9; WISPA Comments at 4.

[102] Blooston Rural Carriers Comments at 2 (discussing "cases where there has been a simple mistake, and data is acquired in good faith by employees or agents but not used improperly or disclosed").

[103] NRECA Reply at 4.

[104] CTIA and NCTA's arguments about the Commission's allegedly overly broad definition of harm to trigger customer notifications of breaches of covered data, and their expressed concerns about excessive reporting to federal agencies, do not account for the fact that this good-faith exception removes an entire category of breaches from the scope of reporting covered by our rules as a threshold matter. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 14-19; NCTA Dec. 5, 2023 *Ex Parte* at 2-3, 5-6. As a result, we are unpersuaded by these parties' cursory claims about possible notice fatigue, consumer confusion or frustration, and interference with data breach investigations. *See* CTIA Dec. 6, 2023 *Ex Parte* at 11, 19.

[105] EPIC et al. Reply at 4-5.

[106] *Id.*

[107] *Data Breach Notice* at 12, 14, paras. 23, 28.

Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni or a successor URL designated by the Wireline Competition Bureau (Bureau). As the Commission found when it adopted the current data breach rules, notifying law enforcement of a breach is consistent with the goal of protecting customers' personal data because it enables such agencies to investigate the breach, "which could result in legal action against the perpetrators," thus ensuring that they do not continue to breach sensitive customer information.[109] The Commission also anticipated that law enforcement investigations into how breaches occurred would enable law enforcement to advise providers and the Commission to take steps to anticipate and prevent future breaches of a similar nature.[110] Our addition of the Commission as a recipient of federal-agency breach notifications is consistent with other federal sector-specific laws, which require prompt notification to the relevant subject-matter agency.[111] As large-scale security breaches resulting from lax or inadequate data security practices and employee training have become more common since the *2007 CPNI Order*, notifying the Commission of breaches will provide Commission staff with important information about data security vulnerabilities and threat patterns that Commission staff can help address and remediate.[112] Commission notification will also shed light on carriers' ongoing compliance with our rules.[113] Consistent with the Commission's proposal and the record in response to the *Data Breach Notice*, we require carriers to notify the Commission of a reportable breach contemporaneously with the Secret Service and FBI.[114]

29. The majority of commenters support including the Commission in data breach notifications.[115] Many of these commenters agree, however, that this new notification requirement should not create new obligations which are duplicative or inconsistent with the preexisting requirement to notify law enforcement agencies, and should instead entail one notification sent to all three.[116] We agree with

(Continued from previous page)

[108] We continue to require carriers to notify the Secret Service and the FBI because doing so enables law enforcement to investigate the breach, "which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI." *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27. Moreover, law enforcement investigations into how breaches occurred would enable law enforcement to advise the carrier and the Commission to take steps to prevent future breaches of that kind. *See id.*; *Data Breach Notice* at 12, para. 24.

[109] *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27.

[110] *Id.* at 6943, para. 27.

[111] *Data Breach Notice* at 12, para. 23; *see, e.g.*, 45 CFR § 164.408; 16 CFR § 318.3(a)(2).

[112] *Data Breach Notice* at 13, para. 24; EPIC Comments at 11.

[113] *Data Breach Notice* at 13, para. 24.

[114] *Id.* at 14, para. 28. As stated in the *Data Breach Notice*, requiring carriers to notify the Commission, Secret Service, and FBI at the same time will minimize burdens on carriers, eliminate confusion regarding obligations, and streamline the reporting process, allowing carriers to free up resources that can be used to address the breach and prevent further harm. Commenters support a single, contemporaneous notification to the Commission, Secret Service, and FBI. *See, e.g.*, ACA Connects Comments at 9; NTCA Comments at 6 ("NTCA does not oppose requiring carriers to report CPNI breaches to the Commission simultaneously with the Secret Service and FBI, provided carriers only need to submit one report and the report can be submitted using the link already provided on the Commission's website for reporting CPNI breaches."); Southern Linc Reply at 5; WTA Comments at 6 (advocating for the same deadline for all federal-agency reports).

[115] *See, e.g.*, ACA Connects Comments at 9; CTIA Comments at 28-29; EPIC Comments at 11; NCTA Comments at 9; NTCA Comments at 6; WTA Comments at 4; NRECA Reply at 3; Southern Linc Reply at 5 (supporting adding the Commission as a recipient of data breach notifications as long as carriers only need to submit one report through a single portal). WISPA opposes contemporaneous notification to the Commission "[i]f the Commission were to require separate notice." WISPA Comments at 8. Because we are not requiring separate notification to the Commission, but are merely adding the Commission as a recipient of breach notifications submitted through the preexisting central reporting facility, we expect that this should allay WISPA's concern.

[116] *See, e.g.*, ACA Connects Comments at 9 (supporting a single notification "disseminated to whichever such entities are designated to receive them"); CTIA Comments at 28-29; Southern Linc Reply at 5.

these suggestions, as we see no need for carriers to file separate or differing notifications to the Commission.[117] As discussed below, we delegate authority to the Bureau to coordinate with the Secret Service to adapt the existing central reporting facility for reporting breaches to the Commission and other federal law enforcement agencies.[118] Additionally, as discussed below, we do not impose differing content requirements for notifications to the different agencies.[119]

30. We disagree with commenters that oppose requiring breach notification to the Commission. For example, ITI and WISPA argue that the existing requirement to notify the Secret Service and the FBI is sufficient, and that notification to the Commission is unnecessary.[120] WISPA also argues that notification to the Commission would hinder law enforcement investigation efforts,[121] and attempts to distinguish the other federal regulations that require notification to sector-specific agencies as less burdensome than the Commission notification we adopt here.[122] We are unpersuaded by these arguments. First, as mentioned above, our requirement to notify the Commission of covered data breaches is necessary to ensure that Commission staff are informed of new types of security vulnerabilities that arise in today's fast-changing data security environment. Additionally, we disagree with WISPA that adding the Commission as a recipient of federal-agency notifications would hinder law enforcement investigation efforts, given the lack of impact the addition will have on the timing, content, or format of notification to the other law enforcement agencies. Indeed, the Secret Service is supportive of the Commission receiving such notifications.[123] Furthermore, our action here avoids adding any additional burden on filers by merely adding the Commission to the list of recipients of the same breach notifications Commission rules already require carriers to submit, and, as discussed in further detail below, further streamlines the filing process by adapting the existing reporting facility for submission.[124] For these reasons, we do not expect carriers of any size to experience increased regulatory burdens as a result of the Commission notification requirement. Moreover, to the extent that carriers are faced with any minimal burdens, such burdens are well justified by the value of these reports to federal law enforcement agencies and the Commission.[125]

2. Threshold Trigger for Federal-Agency Notification

31. We require carriers to inform federal agencies, via the central reporting facility, of all breaches, regardless of the number of customers affected or whether there is a reasonable risk of harm to customers. For breaches that affect 500 or more customers, or for which a carrier cannot determine how many customers are affected, we require carriers to file individual, per-breach notifications as soon as

[117] *See Data Breach Notice* at 13-14, paras. 25, 27.

[118] *See infra* Section III.B.5.

[119] *See infra* Section III.B.4.

[120] ITI Comments at 4; WISPA Comments at 6.

[121] *See* WISPA Comments at 7.

[122] *See id.*.

[123] *See* USSS Letter at 2.

[124] This should also address WISPA's concern that a contemporaneous, but separate, notice to the Commission would impact initial efforts to assess a breach. *See* WISPA Comments at 8.

[125] *See 2007 CPNI Order*, 22 FCC Rcd at 6944, para. 27 ("Notifying law enforcement of CPNI breaches is consistent with the goal of protecting CPNI. Law enforcement can investigate the breach, which could result in legal action against the perpetrators, thus ensuring that they do not continue to breach CPNI. When and if law enforcement determines how the breach occurred, moreover, it can advise the carrier and the Commission, enabling industry to take steps to prevent future breaches of that kind. Because law enforcement will be informed of all breaches, it will be better positioned than individual carriers to develop expertise about the methods and motives associated with CPNI breaches. Again, this should enable law enforcement to advise industry, the Commission, and perhaps Congress regarding additional measures that might prevent future breaches.").

practicable, but no later than seven business days, after reasonable determination of a breach.[126] As we describe below, these notifications must include detailed information regarding the nature of the breach and its impact on affected customers.[127] This same type of notification, and the seven business day timeframe for submission, will also be required in instances where the carrier has conclusively determined that a breach affects fewer than 500 customers unless the carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.[128] For breaches in which a carrier can reasonably determine that a breach affecting fewer than 500 customers is not reasonably likely to harm those customers, we require the carrier to file an annual summary of such breaches via the central reporting facility, instead of a notification.[129] In circumstances where a carrier initially determines that contemporaneous breach notification to federal agencies is not required under these provisions, but later discovers information that would require such notice, we clarify that a carrier must report the breach to federal agencies as soon as practicable, but no later than seven business days of their discovery of this new information.[130]

32. Given our expansion of the definition of "breach" in today's Order to include inadvertent exposure of CPNI and other types of data, allowing carriers to file information regarding smaller, less risky breaches in a summary format on an annual basis will tailor administrative burdens on carriers to reflect those scenarios where reporting is most critical.[131] Our setting of a notification threshold is consistent with many state statutes that similarly do not have an intentionality requirement and require

[126] *See infra* Section III.B.3 (discussing the timeframe requirement for breach notifications to federal agencies).

[127] *See infra* Section III.B.4 (discussing the content requirements for breach notifications to federal agencies).

[128] As discussed below, for breaches affecting fewer than 500 customers and which do not meet the harm-based trigger, we instead require carriers to submit an annual summary of such incidents. *See infra* Section III.B.3.

[129] *See infra* Section III.B.3 (discussing annual reporting requirement for breaches that meet these criteria). To ensure that carriers may be held accountable regarding their determinations of a breach's likelihood of harm and number of affected customers, we require carriers to keep records of the bases of those determinations for two years. *See infra*, Appx. A. We also note that carriers may voluntarily file notification of such a breach in addition to, but not in place of, this annual summary filing.

[130] For example, if a carrier initially determines that federal agency notification within seven business days is not required because a breach affects fewer than 500 customers and harm to customers is not reasonably likely to occur, but later discovers new information suggesting that more than 500 customers were affected, or that harm to customers has occurred, or is likely to occur, as a result of the breach, then the carrier must notify federal agencies as soon as practicable, but no later than within seven business days of this discovery.

[131] *See, e.g.*, CCA Comments at 6 ("[A] numerical threshold similar to those that states have adopted will help carriers efficiently direct their resources and avoid notification fatigue for the Commission, law enforcement, and consumers."); Verizon Comments at 2 ("A threshold trigger would curb excessive reporting and allow authorities to focus resources on more serious breaches with the potential to cause greater harm."); WISPA Comments at 9. We are unpersuaded by NCTA's contention that our rule for data breach reporting to federal agencies is "likely to tax resources and limit the regulator's ability to identify the most problematic practices and act to protect consumers" and result in harm due to lack of harmonization. NCTA Dec. 5, 2023 *Ex Parte* at 3; *see also id*. at 2, 6-7; Letter from Michele K. Thomas, T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, at 5 (filed Dec. 6, 2023) (T-Mobile Dec. 6, 2023 *Ex Parte*) (supporting a harm-based trigger for federal-agency notifications). We are likewise unpersuaded by CTIA's similar contention that "the FCC is not currently equipped to 'become a repository for threat detection and monitoring'" and that the "flood of information threatens to distract FCC and Law Enforcement staff from real and potentially harmful security threats." CTIA Dec. 6, 2023 *Ex Parte* at 15. These parties offer only generalized assertions in that regard without any evidence or analysis demonstrating concrete harms that are likely to result in practice. At the same time, NCTA and CTIA appear to neglect the potential we anticipate for federal agencies to gain useful insight into trends or particular activities that can lead to consumer harm even if, in a given instance, the reported breach happened not to involve consumer harm (whether under the standard set by our rules or in NCTA's and/or CTIA's own subjective judgment).

notice to state law enforcement authorities.[132] Our adoption of a 500-affected-customer threshold is also consistent with an analogous breach of health records notification required by the Federal Trade Commission (FTC).[133]

33. The vast majority of commenters are supportive of the need for a threshold trigger generally,[134] but are divergent regarding what the numerical threshold should be.[135] NCTA supports a threshold of 500 affected customers for federal-agency notifications, noting that such a threshold would "minimize paperwork burdens on providers that wish to focus their resources on protecting customers," and cites a variety of state laws that use that threshold.[136] CTIA and Verizon, however, argue that we should set the threshold to be higher than 1,000 to reflect the larger customer bases of larger carriers.[137] CTIA and Verizon do not provide additional reasoning as to why the size of the carrier's customer base is relevant in determining the threshold for federal-agency notification. If the rationale for adopting a higher threshold for larger carriers is to reduce reporting burdens, we note that larger carriers likely have more resources than smaller carriers to respond to breach incidents. Verizon, for example, admits that it has "a team of more than 1,000 professionals dedicated to implementing corporate-wide security controls and constantly monitoring networks to identify and respond to threats."[138] Additionally, the Commission and other federal law enforcement agencies would likely have an investigative interest in breaches affecting 500 or more customers, regardless of the percentage of the overall customer base those customers represent.

34. We find that the reporting threshold we adopt will both enable the Commission to receive more granular information regarding larger breaches to aid its investigations while also being able to study trends in breach activity through reporting of smaller breaches in annual submissions.[139] Given that a number of states have found such a balance with a 500-affected-customer threshold,[140] our adoption of this threshold also carries the additional benefit of "increas[ing] harmonization with state breach

[132] *See, e.g.*, *Data Breach Notice* at 15, para. 30 nn.75-77; CCA Comments at 6 (supporting a numerical threshold "similar to those that states have adopted"); CTIA Comments at 25 ("[A]dopting a threshold for reporting to the Commission and law enforcement would increase harmonization with state breach notification statutes.").

[133] 16 CFR § 318.5(c); *see* WISPA Comments at 7.

[134] *See, e.g.*, Blooston Rural Carriers Comments at 4; CCA Comments at 6; CTIA Comments at 25; NCTA Comments at 7; NTCA Comments at 5; Verizon Comments at 2, 11-12; WISPA Comments at 9; WTA Comments at 7; NRECA Reply at 4-5; Southern Linc Reply at 6-7; USTelecom Reply at 7; USSS Letter at 2 (suggesting that a specific numerical threshold will "reduce the risks of CPNI breaches," and providing an example of a 500-affected-customer threshold); *see also* EPIC et al. Reply at 22 (taking no position on a threshold trigger, but providing an example of the FTC's proposed Standards for Safeguarding Customer Information which set a threshold of 1,000 impacted consumers to trigger the reporting requirement).

[135] *Compare* NCTA Comments at 7 (advocating for a 500-customer threshold) *with* WTA Comments at 7 (advocating for a 5,000-customer threshold).

[136] NCTA Comments at 8 (citing Cal. Civ. Code § 1798.82(f); Colo. Rev. Stat. §§ 6-1-716(2)(d), (f)(1); Fla. Stat. Ann. §§ 501.171(3)(a), (5)).

[137] CTIA Comments at 24; Verizon Comments at 2, 11-12.

[138] Verizon Comments at 3.

[139] *See* WTA Comments at 7; WTA Reply at 4 ("The critical factor here is not the difference between large and small service providers . . . ."); *accord* Blooston Rural Carriers Reply at 5; *see* NRECA Reply at 4-5.

[140] *See, e.g.*, Cal. Civ. Code § 1798.82(f); Colo. Rev. Stat. § 6-1-716; Del. Code tit. 6, § 12B-102(d); Fla. Stat. § 501.171(3)(a); R.I. Gen. Laws § 11-49.3-4(a)(2).

notification statutes."[141] We therefore also reject rural carriers' suggestion that we adopt a 5,000-affected-customer threshold.[142]

35. Finally, as supported by the record, we apply this threshold trigger only to notifications to federal agencies, and not to customer notifications.[143] Breaches affecting even just a few customers can pose just as much risk to those customers as could breaches with wider impact. For this reason, as discussed above, we continue to require carriers to notify federal agencies within seven business days of breaches that implicate a reasonable risk of customer harm, regardless of the number of customers affected. Doing so will permit federal agencies to investigate smaller breaches where there is a risk of customer harm, and also allow law enforcement agencies to request customer notification delays where such notice would "impede or compromise an ongoing or potential criminal investigation or national security," as specified in our rules.[144]

3. Notification Timeframe

36. We retain our existing requirement that carriers notify federal agencies of a reportable breach as soon as practicable, but no later than seven business days, after reasonable determination of the breach.[145] While the *Data Breach Notice* proposed eliminating the seven business day deadline,[146] based on the record in response, we find that the existing timeframe provides greater certainty for carriers and customers affected by breaches. We agree with ACA Connects that retaining the seven business day deadline properly balances the need to give carriers "reasonable time to prioritize remediation efforts before submitting notifications" with the need to ensure customers receive timely notifications regarding breaches affecting their data.[147] We also agree with NTCA that there is insufficient evidence that the current timeline "is inadequate to accomplish the Commission's goals."[148] Additionally, we agree with NTCA that eliminating the seven business day deadline and only "requiring breaches to be reported 'as soon as practicable' can be interpreted differently by different carriers or even by law enforcement and

[141] CTIA Comments at 25.

[142] *See, e.g.*, WTA Comments at 7; Blooston Rural Carriers Reply at 5.

[143] *See* NCTA Comments at 8 ("[I]t would be reasonable for the Commission to require voice providers to notify affected customers of breaches whenever the harm-based trigger is met, even where less than the threshold minimum number of customers is impacted, so that those customers have the opportunity to prevent or mitigate the harm.").

[144] *See infra* Appx. A.

[145] As commenters point out, in the text of the *Data Breach Notice*, the Commission occasionally used the phrase "after discovery of a breach," rather than "after reasonable determination of a breach" when discussing the appropriate timeframe for federal-agency notification. *See, e.g.*, CTIA Comments at 34-35; ACA Connects Reply at 5; Southern Linc Reply at 6. However, as the Proposed Rules Appendix makes clear, "after discovery" was intended as shorthand, rather than a proposal to substantively change the existing "after reasonable determination of a breach" standard. *See Data Breach Notice* at Appx. A (proposing to require notification to federal agencies "[a]s soon as practicable *after reasonable determination of a breach*") (emphasis added); *see also id*. at 14, para. 28 (seeking comment on "an appropriate timeframe for notifying law enforcement *after reasonable determination* of a CPNI breach," and asking a number of questions about "when a carrier should be treated as having 'reasonably determined' that a breach has occurred") (emphasis added).

[146] *See Data Breach Notice* at 14, para. 28; *id.* at Appx. A.

[147] *See* ACA Connects Comments at 10; *see also* NTCA Comments at 6-7; NTCA Reply at 3-4.

[148] NTCA Comments at 7. Particularly given our historical experience with a seven day deadline, we are unpersuaded by conclusory assertions that meeting that deadline might not always be feasible. *See, e.g.*, CTIA Comments at 34-35 (arguing that the seven business day deadline for federal-agency notifications "is not always feasible or advisable, depending on the complexity of the incident").

the Commission, thereby placing carriers at risk of inadvertently violating the Commission's rules if they construe 'as soon as practicable' differently than the Commission."[149]

37. We disagree with the arguments of other commenters that removing the seven business day deadline is necessary to afford carriers of different sizes and means the flexibility to respond to an evolving breach situation and minimize consumer harm, while also providing accurate and detailed notifications to federal agencies.[150] Carriers have long been subject to the existing seven business day deadline, which was adopted in 2007,[151] and, as EPIC notes, some state jurisdictions require notification to the state attorney general within 3 days.[152] As we point out above, ACA Connects and NTCA—both associations of small-to-medium-sized carriers with presumably fewer resources than larger carriers such as Verizon[153]—support retaining the seven business day time limit. Even assuming, *arguendo*, that the seven business day deadline is a more burdensome or inflexible timeframe for small carriers with "limited personnel and/or resources,"[154] we still find that the countervailing interest in ensuring customers are notified quickly of breaches affecting them outweighs this tailored burden. For this reason, as discussed below, we also remove the seven business day mandatory waiting period between federal-agency notification and customer notification.[155] We lastly clarify that "reasonabl[y] determin[ing]" a breach has occurred does not mean reaching a conclusion regarding every fact surrounding a data security incident that may constitute a breach. Rather, a carrier will be treated as having "reasonabl[y] determin[ed]" that a breach has occurred when the carrier has information indicating that it is more likely than not that there was a breach.

38. While we set this outer bound for federal-agency notifications, we expect that larger carriers with significant resources and staffing will routinely be providing notification of breaches to the Commission well within the seven business day deadline, and that other carriers should strive to do so as well. Indeed, the "as soon as practicable" standard may require such notifications be made in *fewer* days than the seven business day deadline, and a failure to swiftly report breaches may, depending on the circumstances,[156] be untimely and unreasonable, even if within the seven business day deadline. The Enforcement Bureau will continue to investigate carriers that have neglected to provide timely notification to federal agencies after a breach incident pursuant to its delegated authority.

---

[149] NTCA Reply at 4.

[150] *See* Verizon Comments at 6 & n.16; Blooston Rural Carriers Comments at 4; WISPA Comments at 8; Southern Linc Reply at 5-6; USTelecom Reply at 6. Given agencies' ability to calibrate their resources based on the volume of notifications, and our practical experience dealing with investigations at a stage where information might only be preliminary or incomplete, we reject arguments that burdens on the Commission and other law enforcement agencies justify eliminating the seven day reporting deadline. *See, e.g.*, ITI Comments at 3 ("Changing the required reporting time to law enforcement from seven days to 'as soon as practicable' after the discovery of a breach is a workable time frame to prevent overloading regulatory institutions with incomplete or inaccurate information before the incident has been properly analyzed or addressed.")

[151] *2007 CPNI Order*, 22 FCC Rcd at 6944, para. 29.

[152] EPIC Comments at 11.

[153] *See* Verizon Comments at 3 (admitting that it has "a team of more than 1,000 professionals dedicated to implementing corporate-wide security controls and constantly monitoring networks to identify and respond to threats").

[154] Blooston Rural Carriers Comments at 4.

[155] *See infra* Section III.C.2.

[156] For example, if a carrier has made all the determinations necessary to conclude that a breach should be reported to law enforcement after only a few days, it would be inconsistent with the "as soon as practicable" standard for the carrier to wait until the seventh business day—merely because that is the outer limit—before providing the required notice.

39. *Annual Reporting of Certain Small Breaches.* We require carriers to submit, via the existing central reporting facility and no later than February 1, a consolidated summary of breaches that occurred over the course of the previous calendar year which affected fewer than 500 customers, and where the carrier could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach.[157] We delegate authority to the Bureau to coordinate with the Secret Service regarding any modification to the portal that may be necessary to permit the filing of this annual summary. We also delegate authority to the Bureau, working in conjunction with the Public Safety and Homeland Security Bureau, and based on the record of this proceeding—or any additional notice and comment that might be warranted—to determine the content and format requirements of this filing and direct the Bureau to release a public notice announcing these requirements. We instruct the Bureau to minimize the burdens on carriers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. At a minimum, the Bureau should develop requirements that are less burdensome than what is required for individual breach submissions to the reporting facility, and consider streamlined ways for filers to report this summary information. The first annual report will be due the first February 1 after the Office of Management and Budget (OMB) approves the annual reporting requirement under the Paperwork Reduction Act. The first report should cover all breaches between the effective date of the annual reporting requirement and the remainder of the calendar year.[158]

40. We disagree with CTIA's argument that "there is no regulatory goal served by mandating record keeping" for incidents affecting fewer customers than the notification threshold.[159] Breaches that are limited in scope may still reveal patterns or provide evidence of security vulnerabilities at an early stage. As noted in the *Data Breach Notice* and the *2007 CPNI Order*, notification of all breaches, regardless of the number of customers affected or a carrier's determination of harm, "could allow the Commission and federal law enforcement to be 'better positioned than individual carriers to develop expertise about the methods and motives'" associated with breaches.[160] We therefore find that this annual summary of smaller breaches will continue to enable the Commission and our federal law enforcement partners to investigate, remediate, and deter smaller breaches.

41. We also disagree with NTCA and Southern Linc who argue that "requiring carriers to maintain records of any breaches that fall below the notification threshold 'will place an unnecessary burden on carriers . . . .'"[161] On the contrary, we find that any burdens associated with the annual reporting requirement are likely to be well justified by the countervailing benefits discussed above. Nor do commenters objecting to the burden of our rules as unwarranted provide a quantification of their anticipated burdens that would overcome the benefits anticipated from those rules. Moreover, this single annual report containing a summary of such breaches will likely end up replacing numerous smaller breach notifications individually submitted via the central reporting facility throughout the year. Additionally, our rules already require carriers to "maintain a record of all instances where CPNI was

[157] *See Data Breach Notice* at 15, para. 30.

[158] *See* CTIA Dec. 6, 2023 *Ex Parte* at 16-17 (asking that the Commission explicitly state the due date of the first annual report and that such report shall cover "events that occur on or after the effective date of the new rules").

[159] CTIA Comments at 25; *see also* NRECA Reply at 4-5 ("Incidents below [the reporting threshold] likely do not warrant federal government involvement."); Southern Linc Reply at 6-7 (arguing that "requiring carriers to maintain records of any breaches that fall below the notification threshold 'will place an unnecessary burden on carriers . . . .'") (quoting NTCA Comments at 6); CTIA Reply at 16; Letter from Angela Simpson, Senior Vice President & General Counsel, CCA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 2 (filed Dec. 8, 2023) (CCA Dec. 8, 2023 *Ex Parte*). NCTA argues that the annual reporting requirement would "not provide the Commission with meaningful information to serve its goals of identifying data breach patterns," but does not provide more detail as to why such information would not be helpful. NCTA Dec. 5, 2023 *Ex Parte* at 5.

[160] *Data Breach Notice* at 15, para. 30; *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27.

[161] Southern Linc Reply at 6-7 (quoting NTCA Comments at 6).

disclosed or provided to third parties, or where third parties were allowed access to CPNI."[162] The first part of this requirement encompasses all disclosures of CPNI to third parties resulting from a data breach,[163] and thus is broader than the small-breach reporting requirement we adopt today, at least with regard to CPNI.

4. Notification Contents

42. We maintain our existing requirements regarding the contents of data breach notifications to federal law enforcement agencies,[164] with a minor modification as noted below,[165] and apply these same requirements to notifications to the Commission. We agree with comments submitted by WISPA arguing that "the information currently submitted through the FBI/Secret Service reporting facility is largely sufficient and that generally the same information should be reported" under our updated rules.[166] We also take this opportunity to codify these categories of information in our rules to improve the ease of identifying the information that will be needed by regulated entities.[167] Specifically, we require carriers to report, at a minimum, information relevant to the breach, including: carrier address and contact information; a description of the breach incident;[168] the method of compromise; the date range of the incident;[169] the approximate number of customers affected; an estimate of financial loss to the carrier and customers, if any; and the types of data breached.[170] We believe that these disclosures are sufficient to give the Commission and other federal law enforcement agencies the information needed to determine appropriate next steps, such as, for example, conducting an investigation, determining and advising on how such a breach may be prevented in the future, and informing future rulemakings to protect consumers and businesses from harm.[171] Carriers must update their initial breach notification report if: (1) the carrier learns that, in some material respect, the breach notification report initially submitted was incomplete or incorrect; or (2) additional information is acquired by or becomes known to the carrier after the submission of its initial breach notification report.

43. A number of carriers request changes to, or elimination of, certain fields contained in the notification.[172] As discussed below, we are unpersuaded by these arguments, and decline to alter the fields of information collected through the notification portal.

---

[162] 47 CFR § 64.2009(c).

[163] *See also* CTIA Comments at 3-4 ("Verizon maintains records of breaches, notification to law enforcement, and customer notification for at least two years.").

[164] *Data Breach Notice* at 13, para. 27.

[165] *See infra* note 180 (removing field that asks carriers whether there is an extraordinarily urgent need to notify customers before the seven business day waiting period elapses).

[166] WISPA Comments at 7; WTA Comments at 5 (acknowledging that "[m]ost of the Commission's existing requirements regarding the contents of data breach notifications to federal law enforcement agencies are generally reasonable"); *see also* EPIC Comments at 11 (supporting the requirement to share "a detailed description of the breach to the Commission").

[167] *See infra* Appx. A.

[168] *See* EPIC Comments at 11.

[169] *See* EPIC et al. Reply at 22 (supporting requiring an estimated date range of when a security incident occurred rather than requiring providers to determine the precise date).

[170] *See Data Breach Notice* at 13-14, para. 27; *2007 CPNI Order*, 22 FCC Rcd at 6944, para. 29.

[171] *See* EPIC Comments at 11.

[172] ACA Connects Comments at 11-12; CTIA Comments at 30-31; WTA Comments at 5; CTIA Reply at 22-23; *see also* CCA Comments at 7 (stating that, while it "does not take a position on the specific contents that should be included in all notifications to law enforcement, to the Commission, or to customers[,] . . . . [t]he detailed information currently reported to law enforcement for purposes of investigation and potential criminal charges is (continued….)

44. *Customer Billing Addresses.* ACA Connects, CTIA, and WTA request elimination of the requirement to include the billing addresses of affected customers in notifications.[173] ACA Connects states that this reporting requirement has unclear investigative value, and its elimination would "minimize the personal information reported to the Commission and law enforcement agencies."[174] While we acknowledge that federal agencies have been directed to minimize the collection, use, storage, and disclosure of personal information to only that which is relevant and necessary to accomplish an authorized purpose,[175] carriers are not in a position to know, in the absence of input from law enforcement agencies in this proceeding, which fields hold investigative value. Furthermore, because the portal was designed by law enforcement agencies themselves, we must assume that their inclusion of this field reflects a determination that such information holds some investigative value. Finally, we note that the field is not currently marked as a required field. For this reason, the field does not present a reporting burden to carriers, but instead gives carriers an opportunity to provide federal agencies more detail, should they wish to do so or find such detail relevant. WTA argues that "billing names and addresses . . . are not classified as CPNI," and thus should be omitted from the form.[176] Our expansion of covered data to include information beyond CPNI renders this argument moot.[177]

45. *Estimate of Financial Loss.* WTA argues that "estimated financial loss" is "impossible to determine or predict with any degree of accuracy during the brief and chaotic period immediately following discovery of a data breach."[178] We decline to modify or remove this field. While we understand that estimating financial loss is a complex and context-specific calculation, we emphasize the critical importance of this data point in helping federal agencies allocate their resources.[179] Additionally, while carriers should strive to provide in their notifications as accurate a value as possible, we note that even a ballpark estimate or a range of quantities can help agencies determine an incident's priority for the purposes of opening or conducting investigations, and understand the magnitude of future risk posed by certain vulnerabilities.

46. *Other Fields.* CTIA identifies two fields which it argues are no longer necessary given our change to the reporting threshold for federal-agency notifications, as discussed below.[180] Specifically,

(Continued from previous page)
significantly broader than what is necessary and appropriate for the Commission's use. Indeed, over-reporting of such information outside the law enforcement context can introduce additional data-security risks and privacy concerns"). We note that CCA does not provide further detail on "what is necessary and appropriate" in support of its argument or to aid our consideration. *See id.*

[173] ACA Connects Comments at 11-12; CTIA Comments at 31; WTA Comments at 5; CTIA Reply at 22.

[174] ACA Connects Comments at 11-12; *accord* CTIA Comments at 31; *see also* WTA Comments at 5 ("[T]here does not appear to be any need to send [such addresses] to multiple government databases as part of the initial incident notice before law enforcement and other agencies determine whether such addresses are relevant and required for their investigations.").

[175] *See* OMB, To the Heads of Executive Departments and Agencies, *Managing Information as a Strategic Resource*, Circular No. A-130, App. II, Section 3(d) (2016); *see also*, *e.g.*, CCA Comments at 7 ("[O]ver-reporting of [broader than necessary] information . . . can introduce additional data-security risks and privacy concerns."); EPIC et al. Reply at 18 (urging the Commission to "promote the principle of data minimization as a means of ensuring data security").

[176] WTA Comments at 5.

[177] *See supra* Section III.A.1.

[178] WTA Comments at 5.

[179] *See* ACA Connects Comments at 6 n.15; USTelecom Comments at 5.

[180] CTIA Comments at 31. CTIA also requests elimination of the field that asks whether "the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers" before "7 full business days have passed." *Id.* at 31; 47 CFR § 64.2011(b)(1)-(2). CTIA argues that "[r]emoving this field is consistent [with] the (continued….)

CTIA requests that we remove the fields regarding whether the breach "resulted from a change of [a customer's] billing address" or was based on "a personal issue between two individuals."[181] We decline to do so. First, these fields are not marked as "required" on the form, and thus create no burden on reporting carriers that do not wish to complete them, while providing an opportunity for carriers to submit that information where applicable if they find it helpful or appropriate to do so. Second, under our revised rules, a breach stemming from a personal issue between two individuals or a change of a single customer's billing address may still trigger notification to federal agencies. Our reporting threshold only impacts the need to notify federal agencies of breaches affecting fewer than 500 customers that do not implicate harm. As stated below, even small breaches may cause harm for the few customers affected by them.[182]

47. *Harmonizing Reporting Contents with CIRCIA.* In the *Data Breach Notice*, the Commission sought comment on whether we should require telecommunications carriers to report, at a minimum, the information required under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) as part of their notifications to federal agencies.[183] While a few commenters support the alignment or harmonization of these data breach notifications with the requirements under CIRCIA,[184] we decline to take action in this regard at this early stage. CIRCIA directs the Cybersecurity and Infrastructure Security Agency (CISA) to publish a notice of proposed rulemaking implementing its notification provisions by March 15, 2024.[185] The CISA must issue final rules no later than 18 months after the publication of the notice of proposed rulemaking.[186] At the time of this Order, the CISA has not yet released the notice of proposed rulemaking.[187] Therefore, we find it is too early to determine the precise contours of the final reporting requirements, and in the interest of preventing duplicative or inconsistent fields, and consistent with the approach advocated by ACA Connects, Blooston Rural Carriers, and CCA, we will refrain from making additional changes based on CIRCIA and continue to monitor whether such changes may be required in the future.[188]

(Continued from previous page)
NPRM's proposal to eliminate the seven-business-day waiting period." CTIA Comments at 31. We agree with this suggestion as our abrogation of the seven business day waiting period rule will cause such a field to be unnecessary.

[181] CTIA Comments at 31.

[182] *See infra* Section III.B.5.

[183] *Data Breach Notice* at 14, para. 27.

[184] *See, e.g.*, CrowdStrike Comments at 4; ITI Comments at 4, 6.

[185] Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, § 2242(b)(1), 136 Stat. 49, 1044.

[186] *Id.* § 2242(b)(2).

[187] *See* CISA, *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia (last visited Oct. 13, 2023) ("CISA is now reviewing the hundreds of comments received as we start to develop a draft rule. Per the standard rulemaking process, CISA will continue to consult with Federal interagency partners on the draft prior to its publication. CIRCIA requires that CISA publish the draft NRPM before the end of March 2024.").

[188] *See, e.g.*, ACA Connects Comments at 9-10 n.23 ("[A]t this juncture there is no way for the Commission to predict with any certainty whether, and if so to what degree, any revised data breach notification rules the Commission adopts would align with those ultimately adopted by CISA. . . . [T]he substance of the eventual CISA rules is too speculative for the Commission to consider harmonizing its data breach notification rules with CISA's cyber incident reporting rules at this time. Once both agencies adopt their respective incident notification rules, the Commission may further evaluate how to minimize potential duplicate reporting of CPNI breaches arising from cyber incidents, for instance by carving out reporting under the Commission's rules in favor of reporting to CISA where the incident is cyber-based."); Blooston Rural Carriers Comments at 4 (advocating for coordination of our data breach reporting requirements with the CISA "once data breach reporting under the recently-passed [CIRCIA] (continued….)

48. We do not find CTIA's comparison of our reporting trigger to that of the Critical Infrastructure Act of 2022 (CIRCIA) compelling.[189] CIRCIA is concerned with the category of "incidents."[190] CIRCIA does not define "breaches." But under federal guidance to agencies, a breach is a specific type of incident—an incident that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition (etc.) of PII.[191] And it would not be inconsistent for only some incidents to be reportable under CIRCIA but for all breaches to be reportable under our rules. For example, for federal agencies, for an incident to qualify as a "major incident" it must be likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people.[192] But for a "breach" to qualify as a major incident, it can either satisfy that qualitative threshold, *or* it can involve the PII of 100,000 or more people.[193] Thus, the individual privacy concerns implicated by a breach justify a broader reporting trigger.

5. Other Issues

49. *Harm-based Trigger for Federal-Agency Notifications.* In the *Data Breach Notice*, the Commission sought comment on whether to forego requiring notification of a breach to customers or federal agencies in those instances where a telecommunications carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.[194] While we adopt such a harm-based notification trigger for breach notifications to customers generally, as discussed below,[195] we decline to do so for federal-agency notifications of breaches that meet or exceed the 500-affected-customer threshold we describe above.[196] We do not believe that the rationale for adopting a harm-based notification trigger for customer notifications applies in the federal-agency context. Specifically, unlike customers, federal agencies do not have the same vulnerability to notice fatigue, confusion, stress, or

(Continued from previous page)
is in place"); CCA Comments at 3-4 ("The Commission should refrain from needlessly duplicating cyber incident reporting requirements currently being implemented by the [CISA].").

[189] *See* CTIA Dec. 6, 2023 *Ex Parte* at 12.

[190] 6 U.S.C. § 681(3), (5); *see also id.* § 650(12). We also disagree with CTIA's characterization of CIRCIA's incident reporting framework. CTIA argues that CIRCIA's reporting framework "only applies—in a risk-based way—to 'covered cyber incidents,' which must be 'substantial' and do not include all incidents.'" CTIA Dec. 6, 2023 *Ex Parte* at 12. This argument misconstrues the statute. Section 2242(c)(2)(A) of CIRCIA sets a *minimum* on the types of "substantial cyber incidents that constitute covered cyber incidents" and implicitly allows the CISA to expand the definition beyond that in the course of its rulemaking. 8 U.S.C. § 681b(c)(2)(A)(i). For example, one of those required minimums is to report "cyber incident[s] that lead[] to substantial loss of confidentiality, integrity, or availability of such information system or network, or a serious impact on the safety and resiliency of operational systems and processes." *Id.* While a rulemaking implementing CIRCIA is still pending, the CISA may define "loss of confidentiality" to include data breaches. We further note that the two statutory exceptions to "substantial cyber incidents that constitute covered cyber incidents" are narrow, and likely would not prevent the CISA from adopting implementing regulations that broaden the scope of covered cyber incidents that trigger the statute's reporting obligations. *See id.* § 681b(c)(2)(C).

[191] *See* OMB M-17-12, at 9.

[192] OMB M-22-05, at 10.

[193] *Id.* at 11.

[194] *Data Breach Notice* at 10, para. 15.

[195] *See infra* Section III.C.1.

[196] *See supra* Section III.B.2. For breaches that do not meet our reporting threshold of at least 500 affected customers, we do not require notification to federal agencies via the central reporting facility in those instances where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.

financial hardship that would cause the burdens they experience from additional reporting to outweigh the benefits.[197] Additionally, as mentioned above, a report regarding a breach that does not result in harm to customers could nevertheless aid federal agencies in identifying patterns and potential vulnerabilities and develop expertise across the industry.[198] Commenters argue that we should adopt a harm-based notification trigger for all federal-agency notifications to avoid draining carrier resources.[199] While commenters are correct that a general harm-based trigger would likely serve to reduce carriers' reporting burdens, so too would a reporting threshold.[200] We find that our adoption of a reporting threshold is better tailored to reducing carriers' burdens in the federal-agency-notification context while maintaining appropriate benefits of reporting.[201] Our targeted application of a harm-based trigger to breaches affecting fewer than 500 customers ensures that federal agencies are notified before customers and thereby have an opportunity to request a delay if necessary.[202] This trigger also permits federal agencies

[197] *See Data Breach Notice* at 12, para. 20; EPIC et al. Reply at 22 (arguing that a minimum threshold for notification is only appropriate "in the context of reporting to regulators"); *cf.* ACA Connects Comments at 6 (supporting a harm-based notification trigger for federal-agency notifications, but admitting that "federal government entities are not prone to suffer 'notice fatigue' in the same manner as individual consumers"). CTIA argues that by not extending the harm-based trigger to federal-agency notifications, we risk that notifications will "inundate the Commission's breach reporting facility with information" and the "flood of information threatens to distract FCC and Law Enforcement staff from real and potentially harmful security threats." CTIA Dec. 6, 2023 *Ex Parte* at 15. As an initial matter, we note that, as private entities, CTIA and its members lack any particular insight into, or expertise regarding, the administrative burdens affecting federal agencies with respect to these rules. Contrary to CTIA's unsupported assertions, the agencies affected by these breach notification rules do not anticipate significant costs associated with the breach reporting requirements we adopt today. *See* USSS Letter at 2 ("While the Secret Service and FBI are primarily interested in reports related to suspected criminal activity, receiving a broader range of reports through the central reporting facility has not presented substantial costs or challenges."). While we agree that receiving notifications or reports of breaches that carriers have reasonably concluded do not trigger customer notification under the harm-based trigger will require the use of *some* resources by the Commission and law enforcement agencies, we find the value of enabling federal agencies to identify patterns and insecurities and monitor all breaches of covered data outweigh the marginal costs of receiving notifications or reports for breaches that fall in this category.

[198] *Data Breach Notice* at 15, para. 30; *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27.

[199] *See* ACA Connects Comments at 6; Blooston Rural Carriers Comments at 2; CCA Comments at 5; CTIA Comments at 21-22, 27; ITI Comments at 2; NCTA Comments at 1-2; NTCA Comments at 5; Staurulakis Comments at 7; WISPA Comments at 4-5; Blooston Rural Carriers Reply at 2-3; NCTA Reply at 1-2; USTelecom Reply at 3-4; WTA Reply at 3; CTIA Dec. 6, 2023 *Ex Parte* at 15; Letter from Joshua M. Bercu, Vice President, Policy & Advocacy, USTelecom, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 3 (filed Dec. 6, 2023) (USTelecom Dec. 6, 2023 *Ex Parte*).

[200] For our discussion regarding the adoption of a 500-affected-customer threshold for federal-agency notifications, *see supra* Section III.B.2.

[201] Commenters also argue that a harm-based notification trigger is necessary to reduce burdens on government resources. *See, e.g.*, ACA Connects Comments at 6; CTIA Reply at 10; WTA Reply at 3. Even assuming, *arguendo*, that such burdens exist, they would likely be outweighed by the countervailing public interest in federal agencies receiving information concerning all breaches for investigative or trend analysis purposes. Our threshold trigger ensures that federal agencies receive breach information with the appropriate level of detail at the appropriate time given a breach's harmful impact or magnitude.

[202] *See* CCA Comments at 7 ("[I]t is important that the Commission's rules continue to allow law enforcement authorities an opportunity to provide feedback or request a delay of customer notices to allow proper investigation and other appropriate law-enforcement measures.").

to investigate small breaches that are harmful sooner after the breach incident than in a carrier's annual report, as described above.[203]

50. *Method of Notification*. In the *Data Breach Notice*,[204] the Commission proposed to create and maintain a centralized portal for reporting breaches to the Commission and other federal law enforcement agencies. After reviewing the record, we instead require carriers to use the existing data breach reporting facility for notifications to the Secret Service and FBI and delegate authority to the Bureau to coordinate with the Secret Service, the current administrator of the reporting facility, and the FBI, to the extent necessary, to ensure that the Commission will be notified when data breaches are reported and to implement the targeted modifications to the content of breach notifications that we adopt today.[205] Our decision to require the same content and timing for notification to the Commission as we require for notification to the Secret Service and FBI supports the use of a single portal for notifying all three agencies.[206] Consistent with the Secret Service's request,[207] we also delegate authority to the Bureau, working in conjunction with the Public Safety and Homeland Security Bureau and the Office of Managing Director, to collaborate with the Secret Service to explore the possibility of the Commission assuming control and responsibility for the reporting facility in the future, and to transition control of the facility to the Commission should the Bureau and Secret Service agree that such a transition is desirable.

51. Commenters widely supported the use of a single portal for all federal-agency notifications.[208] ACA Connects argues that using the preexisting portal for Commission notification will save government resources that would otherwise be spent developing a redundant portal.[209] NCTA also advocates for the use of the preexisting portal, noting that the portal "works well for service providers."[210] We agree with commenters' analysis and thus require carriers to submit their breach notifications to the Commission and other federal law enforcement agencies through the existing portal. We disagree with John Staurulakis' suggestion that the Commission should instead require carriers to maintain a summary of inadvertent breaches for inclusion in their annual CPNI certification.[211] We find that this approach would significantly delay notification of such breaches to federal agencies, preventing law enforcement from acting quickly to investigate inadvertent breaches that may have widespread, harmful impact on customers.

[203] *See supra* Section III.B.3 (requiring carriers to submit to the Commission and other law enforcement an annual summary of breaches that occurred over the course of the previous calendar year that affected fewer than 500 customers and did not satisfy the harm-based notification trigger).

[204] *Data Breach Notice* at 13, para. 25.

[205] *See, e.g.*, ACA Connects Comments at 10; NCTA Comments at 9; USSS Letter at 2. The existing data breach reporting facility is located at https://www.cpnireporting.gov.

[206] *See supra* Section III.B.4 (discussing adopting the same content requirements for Commission notifications as for notification to other federal agencies); *supra* Section III.B.1 (discussing requiring notifying the Commission contemporaneously with other federal agencies).

[207] USSS Letter at 2 ("[T]he Secret Service supports transitioning operation of the current reporting facility to the FCC.").

[208] *See, e.g.*, Blooston Rural Carriers Comments at 4; CCA Comments at 7; CTIA Comments at 28-29; NTCA Comments at 6; WTA Comments at 4; NRECA Reply at 3.

[209] *See* ACA Connects Comments at 10.

[210] NCTA Comments at 9; *see also id.* at 6 (generally supporting the use of the preexisting portal).

[211] Staurulakis Comments at 5-6.

C. Customer Notification

1. Harm-Based Notification Trigger

52. We adopt a harm-based trigger for notification of breaches to customers so that they may focus their time, effort, and financial resources on the most important and potentially harmful incidents.[212] We agree with commenters that adopting a harm-based trigger serves the public interest by protecting customers from over-notification and notice fatigue, specifically in instances where the carrier has reasonably determined that no harm is likely to occur.[213] As the Commission recognized in the *Data Breach Notice*, it is not only distressing, but time consuming and expensive, to deal with a data breach, costing customers time, effort, and financial difficulty to change their passwords, purchase fraud alerts or credit monitoring, and freeze their credit in instances where the breach is not reasonably likely to result in any harm.[214] Therefore we find that adopting a harm-based notification trigger, along with our expanded definition of breach,[215] will ensure that customers are made aware of potentially harmful instances of breach, whether intentional or not, while preventing unnecessary financial and emotional difficulty in no-harm situations.[216] A harm-based trigger for notification to customers also allows carriers, particularly small and rural providers, to focus their resources on data security and mitigating any harms caused by breaches rather than generating notifications where harm was unlikely.[217] Our decision to adopt a harm-based notification trigger is also consistent with the majority of state laws, which generally do not require covered entities to notify customers of breaches when a determination is made that the breach is unlikely to result in harm.[218]

53. While the record overwhelmingly supports the adoption of a harm-based notification trigger,[219] some commenters worry that such a framework could result in legal ambiguity or lead to

[212] *Data Breach Notice* at 10, para. 15.

[213] *See, e.g.*, NCTA Comments at 1-2; ACA Connects Comments at 5; NRECA Reply at 4; Southern Linc Reply at 3; CTIA Comments at 21-22 ("If notification is required absent a reasonable risk of actual customer harm, customers may be inundated with notifications that are not meaningful or relevant. This poses the real risk of notice fatigue, which could lead to customers not taking notices about potential actual risk seriously."); Letter from Amanda E. Potter, Assistant Vice President – Senior Legal Counsel, AT&T Services, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 3 (filed Dec. 6, 2023) (AT&T Dec. 6, 2023 *Ex Parte*); *see also* NRECA Reply at 4 ("Over-notification risks creating a general numbing effect for consumers, potentially unintentionally promoting less safe consumer behavior. For that reason, NRECA supports other commenters that call for a harm-based trigger for data breach notifications.").

[214] *Data Breach Notice* at 10, para. 16.

[215] We agree with those commenters that argue that the risk of notice fatigue to customers is important in light of our decision to expand the definition of breach. *See, e.g.*, USTelecom Reply at 3; Verizon Comments at 2. Our adoption of the harm-based notification trigger will ensure that customer notification is focused on the incidents which are likely to cause harm, whether the incident was the result of intentional or inadvertent conduct.

[216] *See* WISPA Comments at 4-5 ("A harm-based trigger would tailor the data breach notification rule to situations it is intended to protect—those that could have a harmful impact on consumers.").

[217] Blooston Rural Carriers Comments at 2; WISPA Comments at 5.

[218] *See, e.g.*, Ala. Code § 8-38-5(a); Alaska Stat. § 45.48.010(c); Ariz. Rev. Stat. §18-552(J); Ark. Code § 4-110-105(d); Colo. Rev. Stat. § 6-1-716(2); Conn. Gen. Stat. § 36a-701b(b)(1); *see also Data Breach Notice* at 10, para. 16 n.53; USTelecom Reply at 4; CTIA Reply at 11 ("[E]stablishing a harm-based trigger will align the CPNI rules with the many state data breach notification laws that include harm-based breach notification triggers, furthering harmonization between reporting frameworks."); *cf.* OMB M-17-12, at 29 ("When deciding whether or not to notify individuals potentially affected by a breach, agencies shall consider the assessed risk of harm . . . [which] shall inform the agency's decision of whether or not to notify individuals.").

[219] *See* ACA Connects Reply at 2.

underreporting of breaches.[220] We take several actions to mitigate these concerns. First, we clarify that where a carrier is unable to make a reasonable determination of whether or not harm to customers is likely, the obligation to notify customers remains.[221] Stated differently, we establish a rebuttable presumption of harm and require carriers to notify customers of a breach in situations where the carrier is unable to reasonably determine that harm is reasonably unlikely to occur.[222] Second, as discussed above, we decline to adopt a harm-based trigger for notification to federal law enforcement agencies and the Commission for breaches affecting 500 or more customers. As such, carriers are required to provide notification for *all* incidents which meet the expanded definition of data breach and this affected-customer threshold to federal law enforcement agencies and to the Commission.[223] Moreover, under the rules we adopt today, breaches falling below this threshold must be compiled and reported to federal agencies annually.[224] We believe that this will serve as a backstop to any potential underreporting to customers, as the federal agencies will have an opportunity to act even in instances where the provider may have concluded that harm to the consumer was unlikely.

54. *Evaluating Harm to Customers*. To the extent that a provider has evidence of actual harm to customers, notification is required and the harm-based analysis is conclusive. In instances where there is no definitive evidence of actual harm, as suggested in the *Data Breach Notice*, we identify a set of factors that telecommunications carriers should consider when evaluating whether harm to customers is

[220] EPIC Comments at 8-10; JFL Reply at 3-5. Additionally, EPIC notes that "carriers have a strong incentive to classify any data security incidents they think they can get away with as non-harmful and only admit to harm where the reputational harm (or enforcement penalty) of an exposed cover-up would be greater." EPIC et al. Reply at 19-20.

[221] *Data Breach Notice* at 12, para. 21. In making this determination, we do not require carriers to consult federal law enforcement or the Commission, as suggested by some commenters. *See* ACA Connects Comments at 8. Rather, carriers must determine using the factors outlined below whether harm to customers is likely to occur. If a provider concludes that harm to customers was unlikely and therefore customer notification was not required, but the Commission finds that conclusion to be unreasonable, the Commission will notify the provider.

[222] *See* 45 CFR § 164.402(2) (establishing a rebuttable presumption of a "breach" that triggers the notification requirements under HIPAA except where covered entities demonstrate that there is a low probability that the protected health information in question has been compromised based on a risk assessment of four listed factors). ACA Connects argues that the Commission should decline to establish a rebuttable presumption of consumer harm because having to make filings in the interest of overcoming such a presumption would be burdensome for small providers. ACA Connects Comments at 8. However, we do not require any such filing. Rather, carriers must determine, based on the specific facts of a breach, whether consumer harm is reasonably unlikely to occur. We provide further guidance to carriers on what constitutes harm to consumers below. *See infra* paras. 54-55. We reject NCTA's proposal to limit the rebuttable presumption of harm to "instances where the breach involves a risk of tangible, financial harm, identity theft or theft of service." NCTA Dec. 5, 2023 *Ex Parte* at 5. NCTA's list is underinclusive in that it omits other harms that are significant. Nor does the record enable us to readily draw a line that separates the risks of some harms from others. We clarify that carriers do not need to disprove the potential for each type of harm in every instance to overcome the presumption, but must rather come to a reasonable fact-specific conclusion that, when considering all of the factors as a whole, harm is unlikely to occur.

[223] ACA Connects comments that the harm-based trigger should apply not only to customer breach notifications, but to federal-agency notifications as well. ACA Connects Comments at 6. We disagree. As ACA Connects notes, federal agencies are not prone to notice fatigue in the same way that consumers are. *See id*. Additionally, as discussed above, notifying federal agencies of all breaches allows the Commission and law enforcement agencies to identify patterns and potential vulnerabilities and develop expertise across the industry, thereby enabling them to respond in appropriate and targeted ways. *See Data Breach Notice* at 15, para. 30.

[224] *See supra* Section III.B.3.

reasonably likely.[225] We believe that identifying these factors will promote consistency and further remedy concerns about ambiguity.

55. We find that "harm" to customers could include, but is not limited to: financial harm, physical harm, identity theft, theft of services, potential for blackmail, the disclosure of private facts,[226] the disclosure of contact information for victims of abuse, and other similar types of dangers.[227] Our broad approach to the privacy harms that merit customer notice has ample legal support. First, OMB has noted that "types of harms" that individuals affected by a breach can experience have evolved: "Identity theft can result in embarrassment, inconvenience, reputational harm, emotional harm, financial loss, unfairness, and, in rare cases, risks to public safety."[228] Second, our approach finds support from case law—e.g., decisions holding that reputational harm can confer Article III standing.[229] And third, our approach better reflects consumer expectations than a more cabined-approach to harm: Privacy harms that merit individual notice should be linked to those harms that individuals' experience, not those that carriers can most easily identify.[230]

56. We find that this broader conception of harm is consistent with previous Commission precedent,[231] and we disagree with commenters arguing that "harm" should only include the risk of identity theft or financial harm.[232] We find that adopting such a narrow definition of harm is not only

[225] *Data Breach Notice* at 11, para. 18. WISPA and ACA Connects support the Commission adopting a set of factors to help guide providers in determining whether harm to consumers is reasonably likely. *See* WISPA Comments at 5; ACA Connects Comments at 7. We believe that establishing a set of guidelines and recommendations strikes the right balance between preventing ambiguity, versus adopting a rigid definition which is too inflexible. *Compare* EPIC Comments at 10 (arguing that "any standard based on 'likelihood' of harm is . . . highly malleable") *with* CTIA Comments at 23 ("There is no need for the Commission to identify a set of factors if it clearly defines harm to hone in on actual harm.").

[226] Some parties raise administrability concerns about including harms such as "disclosure of private facts" on the theory that they are too speculative for providers. NCTA Dec. 5, 2024 *Ex Parte* at 5; CTIA Dec. 6, 2023 *Ex Parte* at 18; USTelecom Dec. 6, 2023 *Ex Parte*; AT&T Dec. 6, 2023 *Ex Parte* at 3; CCA Dec. 8, 2023 *Ex Parte* at 2; Letter from Charles R. Moses, President, Ohio Telecom Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 3 (filed Dec. 6, 2023) (Ohio TA Dec. 6, 2023 *Ex Parte*); Letter from Glenn Hamer, President, Texas Association of Business, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 2 (filed Dec. 6, 2023). Beyond this bare assertion, these parties do not meaningfully explain what administrability problems would arise in practice. Additionally, they fail to account for the fact that providers only need make a *reasonable* determination of whether or not harm to customers is likely. Thus, even assuming *arguendo* that particular harms are challenging to evaluate in particular circumstances, a provider is not held to a standard of perfection, and any inherent challenges can be accounted for when evaluating the reasonableness of a given determination.

[227] *Data Breach Notice* at 11, para. 19.

[228] OMB M-17-12, at 7. While OMB was specifically describing harms arising from an identity theft, the fact that those harms go beyond financial supports our conclusion that other types of harm should be considered when assessing the risk of harm from a breach.

[229] *See, e.g.*, *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) ("Various intangible harms can also be concrete. Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion" (citations omitted)).

[230] *See generally* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. 793, 830-861 (2022).

[231] *Data Breach Notice* at 11, n.56.

[232] *See, e.g.*, ITI Comments at 2; ACA Connects Comments at 7; CTIA Reply at 12; WTA Reply at 3-4; CCA Comments at 5 ("The Commission should limit the scope of 'harm' for this purpose to financial harm or identity theft, rather than broader and more amorphous concepts like 'emotional harm,' 'personal embarrassment,' or 'loss of control' over information."); NCTA Dec. 5, 2023 *Ex Parte* at 5; Letter from Michael Romano, Executive Vice

(continued….)

inconsistent with the Commission's longstanding approach, but also could lead to underreporting of breaches, and disregards other important and potentially costly consequences of a breach to customers.[233] While a broader definition of harm may be more difficult for carriers to apply in certain cases, we believe that carriers will be fully capable of understanding when to comply with our disclosure requirements in light of our decision to adopt a rebuttable presumption of harm.

57. When assessing the likelihood of harm to customers, carriers should consider the following factors. Consistent with the *Data Breach Notice*, we find that no single factor on its own is sufficient to make a determination regarding harm to customers.[234]

- **The sensitivity of the information (including in totality) which was breached**.[235] For example, the disclosure of a phone number is less likely to create harm than if the number of calls to that phone number, the duration of those calls, the name of the caller, the content of the conversations, and/or other layers of information is also disclosed.[236] Additionally, harm is more likely if financial information[237] or sensitive personal information[238] was included in the breach. The data's potential for reuse should also be

(Continued from previous page)
President, NTCA – The Rural Broadband Association, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 22-21, at 1 (filed Dec. 6, 2023) (NTCA Dec. 6, 2023 *Ex Parte*). The limited types of harm suggested by these commenters is underinclusive in that it omits other harms that are significant, particularly in the aggregate.

[233] *See* JFL Reply at 5 ("[I]f a harm trigger rule is implemented, the Commission should adopt expansive definitions of harm and breach so that consumers receive notifications about unauthorized access to or use of their information in as many cases as possible. An expansive definition of harm would conform to the word's plain meaning and its ordinary usage and would encompass situations in which some people might reasonably be concerned about possible harm, such as when providers share information with law enforcement representatives or imposters without a lawful order and without following appropriate process."). Blooston Rural Carriers suggests that we adopt a tiered approach to defining harm. Blooston Rural Carriers Comments at 2-3. We believe that a tiered approach would be unnecessarily complicated for carriers to assess the various "levels" of harm. *See* CTIA Reply at 12-13 ("[s]uch an approach would be difficult for carriers to quantify when considering whether access or exposure rises to the level where reporting is required."). Nevertheless, many of the factors that Blooston Rural Carriers suggests as relevant to their proposed analysis (i.e., financial harm, encryption, risk of identity theft) are consistent with the approach that we adopt today.

[234] *Data Breach Notice* at 11, para. 18.

[235] *See* CrowdStrike Comments at 3; OMB M-17-12, at 22 ("Data Elements" and "Private Information"). NCTA proposes an alternative approach under which the rebuttable presumption of harm only would apply "where specific types of data are compromised." NCTA Dec. 5, 2023 *Ex Parte* at 6. But our framework already factors in the sensitivity of the data as part of the overall analysis of harm. And as indicated by our guidance for evaluating harm, we find multiple considerations should be evaluated collectively to accurately gauge the likelihood of consumer harm. Thus, we find that our approach already accounts for potential differences in the risk of harm associated with specific types of data, but does so more effectively than NCTA's proposal by calling for a consideration of the broader relevant context, as well.

[236] This contextual approach to gauging the sensitivity of customer information is consistent with the definition of PII we adopt above with respect to our breach notification rules, which considers whether information is disclosed in combination with other information which inherently increases the risk associated with the disclosure. *See supra* Section III.A.1 (breach notification requirements directed at disclosure of "first name or first initial, and last name, *in combination with* any government-issued identification numbers," or "user name or e-mail address, *in combination with* a password or security question and answer") (emphasis added).

[237] Commenters agree that a breach implicating financial information is likely harmful. *See* Blooston Rural Carriers Comments at 3; NTCA Comments at 5; Southern Linc Reply at 3-4.

[238] Some data elements are always considered sensitive, such as bank account numbers and Social Security Numbers. Other data elements (e.g., Date of Birth) become sensitive when paired with another data element (e.g., name, address, or phone number). And still other data elements may be sensitive in context (e.g., data identifying a subscriber in a TRS program, because confirmed participation may be sufficient to reveal an individual's hearing- or (continued….)

considered. For example, if a password is compromised, it is possible that the information could be reused to attack other accounts. Finally, if information is not able to be changed, it is more sensitive than information that is changeable. For example, a customer could change their password for an account, but the customer is unable to change their social security number, for instance.

- **The nature and duration of the breach**.[239] For example, if the information was widely accessible online over a long period of time, harm is more likely than if the information was only briefly accessible to a limited number of individuals. Information on a portable USB flash drive which does not require any special skill or knowledge to access is more likely to cause harm than information on a secured back-up device which is password protected. Covered data that was exposed for an extended period of time is more likely to have been accessed or used to the detriment of customers than data that was only briefly exposed.
- **Mitigations**.[240] How quickly the carrier discovered the breach, and whether it took actions to mitigate any potential harm to the customers, is also a factor.
- **Intentionality**.[241] In the case of an individual or entity intentionally obtaining access to covered data, such as by using the practice of pretexting, unauthorized intrusion into a physical or virtual space, theft of a device, or other similar activities, harm is more likely to occur. Conversely, an accidental breach, such as that resulting from a misdirected email, accidentally losing a device with covered data stored on it, or other similar activities, is less likely to result in harm.

58. *Encryption Safe Harbor*. As requested by a number of parties, we adopt a safe harbor under which customer notification is not required where a breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed.[242] For the purposes of this safe harbor, we define encrypted data as covered data that has been transformed through the use of an algorithmic process into a form that is unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.[243] We agree with commenters that the risk of harm to customers is significantly reduced when the data was encrypted,[244] provided that the carrier has evidence that the encryption key has not been compromised.[245]

(Continued from previous page)
speech-related disability). Consistent with the approach we take in this order, carriers must consider each element and all of the elements taken together, in context, to determine whether sensitive information was revealed in a breach.

[239] OMB M-17-12, at 23-25 ("Permanence," "Format and Media," and "Duration of Exposure").

[240] *See* CrowdStrike Comments at 3; 45 CFR § 164.402(2)(iv).

[241] OMB M-17-12, at 26 ("Intent").

[242] Comments in the record support establishing a notification exception for encrypted data. *See, e.g.*, NCTA Reply at 5; Sorenson Comments at 4; NCTA Dec. 5, 2023 *Ex Parte* at 6; USTelecom Dec. 6, 2023 *Ex Parte* at 3; AT&T Dec. 6, 2023 *Ex Parte* at 3; T-Mobile Dec. 6, 2023 *Ex Parte* at 5.

[243] *See* Appx. A.

[244] CTIA Comments at 23; Blooston Rural Carriers Comments at 2-3.

[245] While EPIC recommends that the Commission not exempt breaches solely involving encrypted data from its breach notification rules, EPIC does nonetheless acknowledge that "a typical breach of encrypted data may present a lower risk of harm to consumers", though "encrypted data can nevertheless be compromised if a third party obtains access to the requisite encryption keys or is able to identify and exploit an additional security vulnerability." EPIC Comments at 9. We agree. For those reasons, encrypted data is only exempted from the customer breach notification requirement where the carrier has definitive evidence that the encryption key was not compromised. Additionally, whether data was encrypted or not is irrelevant to the federal-government breach notification

(continued….)

We also agree with commenters that our decision to implement a notification exception for encrypted data will incentivize and encourage the use of encryption to the benefit of the public,[246] and further the goal of harmonization with state and other laws.[247] To the extent that a threat actor appears to have circumvented encryption, however, the carrier should conduct a harm-based analysis as if the data was never encrypted.

2. Customer Notification Timeframe

59. Consistent with the Commission's proposal in the *Data Breach Notice*,[248] we require telecommunications carriers to notify customers of covered data breaches without unreasonable delay after notification to federal agencies. We find that the current framework, which imposes a mandatory seven business day waiting period, is out-of-step with current approaches regarding the urgency of notifying victims about breaches of their personal information,[249] and that the public interest is better served by eliminating the waiting period and thereby increasing the speed at which customers can receive the important information contained in a notice.[250] At the same time, we recognize the importance of law enforcement's ability to investigate a breach, and understand that in certain situations, notification of a breach may interfere with a criminal investigation or national security.[251] Therefore, consistent with the

(Continued from previous page)
requirement. As such, carriers are still required to report *all* breaches of covered data, whether that data was encrypted or not, to the Commission and law enforcement agencies. As we have previously explained, data regarding breaches, even breaches with little or no risk of consumer harm, can be helpful to assist federal agencies to determine data security vulnerabilities and threat patterns. Stated differently, encryption does not exempt an incident from the Commission's definition of breach, but rather only limits the instances where notification to a customer may be necessary.

[246] CTIA Reply at 14; NCTA Dec. 5, 2023 *Ex Parte* at 6-7; CTIA Dec. 6, 2023 *Ex Parte* at 20-21.

[247] CTIA Dec. 6, 2023 *Ex Parte* at 20-21. Several states have established an exception for encrypted data from their breach notification requirements so long as the key has not been compromised or also breached. *See* Cal. Civ. Code § 1798.82(a) (unless "encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable"); Colo. Rev. Stat. § 6-1-716(a.4) (unless "the confidential process, encryption key, or other means to decipher the secured information was also acquired in the security breach or was reasonably believed to have been acquired"); 9 GCA § 48.30(a)-(b) (unless "encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any resident of Guam"); Mich. Comp. Laws § 445.72(1); Okla. Stat. tit. 24 § 163(A)-(B); 73 Pa. Stat. § 2303(b); S.D. Cod. Laws § 22-40-19(1); Va. Code § 18.2-186.6(C); Wash. Rev. Code § 19.255.010(1); W.V. Code § 46A-2A-102(a)-(b). Additionally, in recent amendments to the Gramm-Leach-Bliley Act's Safeguards Rule, the FTC exempted encrypted data from its notification requirement. *See Standards for Safeguarding Customer Information*, Final Rule, 88 Fed. Reg. 77,499, 77,503 (Nov. 13, 2023).

[248] *Data Breach Notice* at 15-16, para. 31.

[249] *Id.* at 16, para. 32.

[250] Consumer Groups Comments at 2; CTIA Comments at 19-20; ITI Comments at 3; NCTA Comments at 3; USTelecom Comments at 6; Verizon Comments at 1 ("[T]he Commission should adopt its proposal to eliminate the existing seven-day customer notification rule. This rule harms consumers by delaying their ability to take steps to protect themselves in the event of a breach involving their customer proprietary network information ('CPNI'). The Commission should amend the rule, as proposed, so that providers may notify customers of breaches without unreasonable delay.").

[251] *See Data Breach Notice* at 16, para. 31 (citing *2007 CPNI Order*, 22 FCC Rcd at 6943-44, para. 28); *see also* CCA Comments at 7 ("CCA agrees that a strict rule requiring a delay of at least seven business days after notification to law enforcement is unnecessary. That said, it is important that the Commission's rules continue to allow law enforcement authorities an opportunity to provide feedback or request a delay of customer notices to allow proper investigation and other appropriate law-enforcement measures.").

Secret Service's request,[252] we will allow law enforcement to request an initial delay of up to 30 days[253] in those specific circumstances where one is warranted.[254]

60. We find that the "without unreasonable delay" standard encourages carriers to promptly notify customers of covered data breaches while offering the flexibility to be responsive to the specifics of a situation.[255] This approach is consistent with many existing data breach notification laws that require expedited notice but refrain from requiring a specific timeframe.[256] As suggested by commenters, the "without unreasonable delay" standard could take into account factors such as the provider's size, as a small carrier may have limited resources and could require additional time to investigate a CPNI data breach than a larger carrier.[257]

61. In order to ensure that carriers notify customers quickly even in complex situations,[258] we require customer notification no later than 30 days after reasonable determination of a breach.[259] The 30-day maximum amount of time is consistent with many existing state laws.[260] Some commenters request that the Commission adopt a safe-harbor for customer notification after determination or discovery of a

[252] *See* USSS Letter at 2 (supporting the continued ability for law enforcement to request a delay of customer notification).

[253] CTIA Comments at 20.

[254] WISPA commented that the seven business day waiting period can be "crucial for law enforcement to effectively investigate the breach." WISPA Comments at 9. We agree that law enforcement requires an opportunity to investigate a breach, but do not find that a seven business day waiting period, applied to all breaches, is necessary. Under the framework that we adopt today, law enforcement may request a delay when one would be useful, but in the many circumstances where a delay is not necessary, this rule will allow carriers to more promptly notify customers, thereby empowering them to take action to mitigate any harms.

[255] NCTA Reply at 2; ITI Comments at 3; WISPA Comments at 9-10; Southern Linc Reply at 7.

[256] *See Data Breach Notice* at 16, para. 33 (citing 12 CFR pt. 364, Appx. B, Supp. A § III(A)(1) (interpreting GLBA § 501(b)); Cal. Civ. Code § 1798.29(a); Va. Code Ann. § 18.2-186.6(B) ("without unreasonable delay"); D.C. Code § 28-3852(a) ("in the most expedient time possible and without unreasonable delay"); Wyo. Stat. Ann. § 40-12-502(a) ("notice shall be made in the most expedient time possible and without unreasonable delay"); FTC, Data Breach Response: A Guide for Business at 6 (2021), https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf (FTC Data Breach Guide)); *see also* USTelecom Comments at 7.

[257] ACA Connects Comments at 14; Blooston Rural Carriers Comments at 5-6; Blooston Rural Carriers Reply at 3 ("A reasonableness timeframe will allow service providers to respond more quickly when circumstances warrant, while at the same time allowing flexibility if a small service provider has limited personnel and/or resources available and is focused on addressing and minimizing harm to consumers.").

[258] While in many circumstances, the "without unreasonable delay" standard means that the customer will be notified in less than seven business days, we note that in some circumstances, this standard may lead to a longer waiting time than the previous seven days. *See, e.g.*, USTelecom Reply at 6 ("[A]llowing carriers to fully investigate an incident before providing notice of the breach reduces the risk of inaccurate or incomplete information. It also avoids circumstances in which premature customer notice could lead to further harm, such as when the breach is a result of a cybersecurity vulnerability. The Commission therefore should adopt its proposals to require providers to notify customers of breaches without unreasonable delay . . . after reasonable determination of a breach."). For that reason, we adopt the 30-day back-stop in order to prevent unnecessarily long delays, even in such instances as the one described by USTelecom, where the carrier is engaged in investigations of the incident.

[259] *Data Breach Notice* at 17, para. 34.

[260] *Id.* at 17, para. 34 (citing Colo. Rev. Stat. § 6-1-716; Fla. Stat. § 501.171(4)(a); Wash. Rev. Code § 19.255.010(8)). In the *Data Breach Notice*, we also considered adopting an "outside limit" of 45 or 60 days after discovery of a breach. *Id*. However, we find that 30 days offers providers enough flexibility while recognizing the urgency of notifying customers as quickly as possible and without unnecessary delays.

breach.[261] We decline to adopt such a safe harbor because we encourage providers to notify customers as quickly as possible in each individual instance. However, we do establish a requirement that carriers notify customers no later than 30 days after reasonable determination of a breach to provide a clear outer bound to the "without unreasonable delay" standard.[262]

3. Other Issues

62. *Content of Customer Breach Notification*. Consistent with our current rules, we decline to adopt specific minimum categories of information required in a customer breach notification.[263] We make clear, however, that a notification must include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. While all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have laws requiring private or governmental entities to notify individuals of breaches involving their personal information, not all of those entities impose minimum content requirements for those notices.[264] We agree with NTCA that adding requirements with the potential to differ from other customer notice requirements imposed by states or otherwise may create unnecessary burdens on carriers, particularly small ones,[265] as well as confusion among customers.[266] We also find persuasive arguments by commenters that specifying the required content of customer notifications beyond the basic standard described above would prevent carriers from having enough flexibility[267] to craft notifications that are more responsive to, and appropriate for, the specific facts of a breach, the customers, and the carrier involved.[268] Finally, imposing minimum requirements may delay a carrier's ability to timely notify customers, as it may take time to gather all of the necessary details and information even where it would be in the customer's best interest to receive notification more quickly albeit with less detail.

63. Instead, we adopt as recommendations[269] the following categories of information in security breach notices to customers: (1) the estimated date of the breach;[270] (2) a description of the customer information that was used, disclosed, or accessed; (3) information on how customers, including

[261] *See* CTIA Comments at 35-36 (requesting a 45-day safe harbor); WTA Comments at 6-7 (requesting a 60-day safe harbor).

[262] *See* ACA Connects Comments at 14 (requesting Commission guidance as to the potential outer bounds of 'without unreasonable delay').

[263] *Data Breach Notice* at 18, para. 38.

[264] *See id.* at 19, para. 39; *see also* Blooston Rural Carriers Comments at 6 ("While some state laws specify minimum notice requirements, other states do not and the Commission should avoid adopting notice requirements that are more stringent than what individual states require.").

[265] NTCA Comments at 8; NTCA Reply at 6; USTelecom Comments at 8.

[266] CTIA Comments at 31-32.

[267] Southern Linc Reply at 7-8; USTelecom Comments at 2; Verizon Comments at 1; CTIA Reply at 23.

[268] CTIA Comments at 31-33; USTelecom Reply at 6. We find this argument particularly persuasive as it relates to small and rural carriers. *See* Staurulakis Comments at 6-7; Blooston Rural Carriers Reply at 4 ("Small and rural service providers have a strong connection to their customers and communities and should continue to have discretion to tailor notifications to the precise circumstances and to their customers' needs.").

[269] Beyond the basic standard set by our rules, we agree with commenters that adopting *guidance* (rather than *requirements*) fosters the goal of ensuring that the customer has access to pertinent information about a breach while affording carriers flexibility to tailor the contents of a customer notification to the specific circumstances at hand. ACA Connects Comments at 15.

[270] We agree with some commenters that carriers may not know, with certainty, the precise date of a breach. *Id.* at 16; NTCA Comments at 8. For that reason, we have modified this requirement from our original proposal by suggesting the estimated date of the breach.

customers with disabilities, can contact the carrier to inquire about the breach; (4) information about how to contact the Commission, FTC, and any state regulatory agencies relevant to the customer and the service; (5) if the breach creates a risk of identity theft,[271] information about national credit reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the carrier is offering to affected customers; and (6) what other steps customers should take to mitigate their risk based on the specific categories of information exposed in the breach.[272] We believe that adopting recommendations will further the goals of consistently and sufficiently notifying customers of data breaches while maintaining some flexibility for carriers to tailor each notification to the specific facts and details of the breach.[273]

64. *Method of Customer Breach Notification*. We decline to specify at this time the method of customer breach notification, and instead allow the carriers to assess for themselves how to best notify their customers of a data breach incident.[274] Generally, carriers have pre-established methods of communicating with their customers about other important matters related to their service, such as outages and scheduled repairs.[275] These methods may differ among carriers based on their size, their unique relationship with their customers, the types of customers impacted, and other factors.[276] Therefore, we find that maintaining flexibility in the method of customer breach notification both reduces the burden on the carriers and prevents customer confusion that could arise if carriers were required to provide disclosures in a way that differed from how customers were used to receiving important information from their carriers.[277]

D. TRS Breach Reporting

65. In 2013, the Commission adopted privacy rules applicable to telecommunications relay services (TRS) providers, to protect the CPNI of TRS users.[278] In doing so, the Commission found that

[271] Breaches which involve data such as a social security number, birth certificate, taxpayer identification number, bank account number, driver's license number, and other similar types of personally identifiable information unique to each person create the highest level of risk of identity theft. *See* Am. Bar Ass'n, *Identity Theft and Fraud: How to Evaluate and Manage Risks* (Mar. 2020), https://www.americanbar.org/news/abanews/publications/youraba/2020/youraba-march-2020/identity-theft-and-fraud. While breaches involving the types of data listed here should be considered to create a risk of identity theft for customers, this is not an exclusive list and should not be considered as such. There may be other types of data not listed here that, either alone or in conjunction with other data, may potentially create a risk of identity theft for customers.

[272] *Data Breach Notice* at 20, para. 40.

[273] While some commenters such as EPIC suggest that the Commission should adopt minimum content requirements, we believe that adopting recommendations furthers the same objective of "inform[ing] the consumer of the risks they face but also equip[ping] the consumer with options for immediate steps to reduce the downstream harms that may result" while also maintaining the flexibility that commenters overwhelmingly noted was important for effectively and quickly notifying customers. EPIC Comments at 8; *see also* JFL Reply at 6-7; WISPA Comments at 10.

[274] *Data Breach Notice* at 20, para. 41.

[275] Blooston Rural Carriers Comments at 6.

[276] CCA Comments at 8 (noting that a carrier may communicate differently, for example, with residential customers versus business customers); CTIA Reply at 24.

[277] USTelecom Comments at 2.

[278] *2013 VRS Reform Order*, 28 FCC Rcd at 8680-87, paras. 155-72; 47 CFR §§ 64.5101-64.5111. The adopted rules apply to all forms of TRS and point-to-point service over the facilities of a video relay service (VRS) provider using VRS access technology. Point-to-Point service is not compensated on a per-minute basis, because such calls are not relayed with the assistance of a communications assistant or technological equivalent, but are an essential aspect of ensuring individuals who are deaf, hard of hearing, deafblind, or who have a speech disability engage in (continued….)

"for TRS to be functionally equivalent to voice telephone services, consumers with disabilities who use TRS are entitled to have the same assurances of privacy as do consumers without disabilities for voice telephone services."[279] The privacy rules for TRS include a breach notification rule that is equivalent to section 64.2011 in terms of the substantive protection afforded to TRS users.[280]

66. To maintain functional equivalency, we amend section 64.5111 so that it continues to provide equivalent privacy protection for TRS users in line with our amendments to section 64.2011. Thus, in this Order we apply our breach notification and reporting obligations for TRS providers to covered data, including PII and CPNI. We also expand the definition of "breach" in section 64.5111 to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a TRS provider, and such information is not used improperly or further disclosed. We also require TRS providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable, and in no event later than seven business days, after reasonable determination of a breach, except in cases where a breach affects fewer than 500 individuals, and a provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.[281] Any breach affecting fewer than 500 individuals where there is no reasonable likelihood of harm to customers must be reported simultaneously to the Commission, Secret Service, and FBI in a single, consolidated annual filing. We further revise our rules to require TRS providers to report breaches to the Commission, Secret Service, and FBI contemporaneously via the existing centralized portal that providers already use and with which they are familiar. In terms of the content of such notifications, we mandate that notifications to the Commission, Secret Service, and FBI must, at a minimum, include: TRS provider address and contact information; a description of the breach incident; a description of the customer information that was used, disclosed, or accessed; the method of compromise; the date range of the incident and approximate number of customers affected; an estimate of the financial loss to providers and customers, if any; and the types of data breached. More specifically, we clarify that, if any data, whether partial or complete, on the contents of conversations is compromised as part of a breach—such as call transcripts—the compromise must be disclosed as part of the notification to the Commission, Secret Service, and FBI.

67. Regarding breach notifications furnished to TRS users, we introduce a harm-based trigger and eliminate the requirement to notify TRS users of a breach in those instances where a TRS provider can reasonably determine that no harm to TRS users is reasonably likely to occur as a result of the breach. We further revise our rules to eliminate the mandatory seven business day waiting period to notify TRS users and instead require TRS providers to notify TRS users of breaches without unreasonable delay after notification to law enforcement, and in no case later than 30 days after reasonable determination of a breach, unless law enforcement requests a longer delay. We also recommend minimum categories of information for inclusion in TRS user notifications. Notifications shall be provided in formats that are accessible to individuals with disabilities.

(Continued from previous page)
communication in a manner that is functionally equivalent to the ability of a hearing individual who does not have a speech disability to communicate using voice communication services. *See* 47 U.S.C. § 225(a)(3).

[279] *2013 VRS Reform Order*, 28 FCC Rcd at 8683, para. 164.

[280] The texts of the two provisions are virtually identical, except for the substitution of the term "TRS provider" for "telecommunications carrier" in section 64.5111. *Compare* 47 CFR § 64.2011 *with id.* § 64.5111. The only substantive difference is that under the TRS rule, after a TRS provider notifies law enforcement of a breach, it "shall file a copy of the notification with the Disability Rights Office of the Consumer and Governmental Affairs Bureau at the same time as when the TRS provider notifies the customers." *Id.* § 64.5111(a).

[281] As with our breach reporting rules for telecommunications carriers, where a TRS provider is unable to reasonably determine that no harm to consumers is reasonably likely to occur as a result of the breach, it must promptly notify the relevant federal agencies regardless of the size of the breach. *See supra* Section III.C.1.

68. As with our revisions to section 64.2011, we find that these changes will best protect and inform TRS users without resulting in overreporting or excessively burdening TRS providers or federal agencies. These changes to our rules will also allow the Commission and its law enforcement partners to receive the information they require in a timely manner so that they can mitigate the harm and fallout of breaches while also taking action to deter future breaches.

1. Defining "Breach"

69. In this section, we apply our breach notification and reporting obligations for TRS providers to covered data, including PII and CPNI. We also take the opportunity to emphasize that covered data under the TRS data breach notification rule includes call content given the unique concerns that arise with respect to call content in the TRS context. And, we expand the definition of "breach" in section 64.5111 to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a TRS provider, and such information is not used improperly or further disclosed.

70. *Covered Data*. Consistent with the provisions we adopt above for carriers, we apply our breach notification and reporting obligations for TRS providers to covered data, including PII and CPNI.[282] We do so for the reasons discussed above with respect to our breach notification and reporting obligations for carriers.[283] In addition, as discussed below,[284] section 225 of the Act directs the Commission to ensure that TRS are available to enable communication in a manner that is functionally equivalent to voice telephone services.[285] The Commission has found that applying the privacy protections of the Commission's regulations to TRS users advances the functional equivalency of TRS.[286] In order to ensure the functional equivalency of TRS, and to ensure that TRS users enjoy the same protections as customers of telecommunications carriers and interconnected VoIP providers, we apply our TRS data breach obligations to the same scope of customer information, including both PII and CPNI. We also incorporate, by reference, the scope of covered PII adopted above, for the same reasons as discussed above.[287]

71. We disagree with Hamilton Relay that the "assurances of privacy" that TRS users can expect "are limited to CPNI and should not be extended to other elements of personal information, including sensitive personal information."[288] In the *Data Breach Notice*, the Commission recognized that providers possess proprietary information of customers other than CPNI, which customers have an interest in protecting from public exposure.[289] This interest is particularly acute in the case of TRS users. TRS providers have access to the contents of customers' conversations, and, as AARO notes, any potential disclosure of TRS conversation content is a "grave privacy concern."[290] While section 225 and our TRS rules generally prohibit TRS providers from disclosing the content of any relayed conversation and from keeping records of the content of any such conversation beyond the duration of the call, that prohibition is not sufficient to protect TRS users from risks that may arise from data breaches.[291] For

[282] *See supra* Section III.A.1; *infra* Appx. A (47 CFR § 64.5111(e) (defining "breach" for TRS providers).

[283] *See supra* Section III.A.1.

[284] *See infra* Section III.E.4.

[285] 47 U.S.C. § 225(a)(3), (b)(1).

[286] *2013 VRS Reform Order*, 28 FCC Rcd at 8685-86, para. 170.

[287] *See supra* Section III.A.1.

[288] Hamilton Relay Comments at 9.

[289] *Data Breach Notice* at 12, para. 22.

[290] AARO Comments at 2.

[291] 47 U.S.C. § 225(d)(1)(F); 47 CFR § 64.604(a)(2)(i). Section 64.604(a)(2)(i) of our rules generally includes an exception where "authorized by section 705 of the Communications Act, 47 U.S.C. 605," and "a limited exception (continued….)

instance, if a breach were to expose transcripts of TRS calls that were in progress at the time of the breach, the breaching party could obtain conversation contents between a TRS user and medical professionals, romantic partners, family members, friends, or professional colleagues, and as such may include sensitive details, such as a user's medical history, disability status, financial situation, political views, relationship status and dynamics, and religious beliefs.[292] The disclosure of such information could lead to serious consequences, including embarrassment, ostracization from family and friends, and extortion by the breaching party or others who have gained access to the information.[293]

72. Indeed, information about call content is not commonly available to traditional voice service providers, and thus traditional voice service customers do not face the same privacy risks in this regard as TRS users. As a result, it is particularly important in the TRS context that we emphasize the need for breach notifications with respect to call content.[294] Consistent with the congressional directive that the Commission's TRS rules guard against the disclosure of call content,[295] and to promote functional equivalence between TRS and traditional voice communications services,[296] we therefore make explicit in the text of section 64.5111 of our rules that a breach involving call content implicates those notification requirements.

73. Just as with telecommunications carriers, we believe that the unauthorized exposure of sensitive personal information that the provider has received from the customer or about the customer in connection with the customer relationship (e.g., initiation, provision, or maintenance, of service) is reasonably likely to pose risk of customer harm. Accordingly, any unauthorized disclosure of such information warrants notification to the customer, the Commission, and other law enforcement.[297] Consumers expect that they will be notified of substantial breaches that endanger their privacy, and businesses that handle sensitive personal information should expect to be obligated to report such breaches.[298]

74. We further disagree with Hamilton Relay's assertion that our privacy authority does not extend to other elements of personal information beyond CPNI, or that doing so would be inconsistent with the plain language of the Act or result in duplicative or inconsistent requirements between Commission rules and state laws.[299] We do so for the reasons discussed above,[300] and because of the

(Continued from previous page)
for STS CAs," who "may retain information from a particular call in order to facilitate the completion of consecutive calls, at the request of the user." 47 CFR § 64.604(a)(2)(i).

[292] AARO Comments at 2-3.

[293] *Id.* at 3.

[294] CPNI, PII, and the contents of calls are non-exclusive, and potentially overlapping, categories of information. *See supra* para. 17 (noting, for example, that CPNI is a subset of PII).

[295] 47 U.S.C. § 225(d)(1)(F).

[296] *Id.* § 225(a)(3); *see also id.* § 225(d)(1)(A) (directing the Commission to "establish functional requirements, guidelines, and operations procedures for telecommunications relay services").

[297] *See supra* Section III.A.1.

[298] *See, e.g.*, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et al.*, CG Docket No. 02-278 et al., Declaratory Ruling and Order, 30 FCC Rcd 7961, 8025, para. 132 (2015) (Calls reporting data breaches or conveying remediation information following a breach are "intended to address exigent circumstances in which a quick, timely communication with a consumer could prevent considerable consumer harms from occurring or, in the case of the remediation calls, could help quickly mitigate the extent of harm that will occur."); *TerraCom NAL*, 29 FCC Rcd at 13340-41, para. 43 ("We expect carriers to act in an abundance of caution . . . in their practices with respect to notifying consumers of security breaches.").

[299] Hamilton Relay Comments at 9.

[300] *See supra* Section III.A.1.

principle of functional equivalency. By ensuring that the same data breach notification requirements we apply to traditional telecommunications carriers also apply to TRS providers, we advance the interest of ensuring that consumers can have the same expectations regarding services that they view as similar. Thus, the approach we adopt today not only reflects the practical expectations of consumers but also honors the intention of Congress.[301]

75. EPIC concurs with this approach.[302] We note that covered data would include PII that a TRS provider collects to register a customer in the TRS User Registration Database in order to provide services.[303] In November 2021 and March 2022 orders revoking the operating authority of certain telecommunications carriers, the Commission further stated that all communications service providers have "a statutory responsibility to ensure the protection of customer information, including PII and CPNI."[304]

76. Because TRS providers have access to proprietary information of customers other than CPNI, and customers have an interest in protecting that information from public exposure, we find that TRS providers should be obligated to comply with our breach notification rule whenever customers' personally identifiable information is the subject of a breach, whether or not the information is CPNI.

77. *Inadvertent Access, Use, or Disclosure*. We expand the definition of "breach" in section 64.5111 to include inadvertent access, use, or disclosure of covered data, except in those cases where such information is acquired in good faith by an employee or agent of a TRS provider, and such information is not used improperly or further disclosed.[305] Section 64.5111(e) of our rules currently defines a breach more narrowly as occurring "when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI."[306] As noted above, this construction was adopted in response to the practice of pretexting.[307] As discussed above, in the years since, numerous data breaches have shown that the inadvertent exposure—as much as intentional exposure—of customer information can and does result in the loss and misuse of sensitive information by scammers, phishers, and other bad actors, and can thus trigger a need to inform the affected consumers so that they can take appropriate action to protect themselves and their sensitive information.[308] Whether a breach was intentional may not be readily apparent, and continuing to require disclosure of only intentional breaches could thus lead to underreporting. It is moreover critical that the Commission and law enforcement be made aware of any unintentional access, use, or disclosure of covered data so that we can investigate and advise TRS providers on how best to avoid future breaches and so that we are prepared and ready to investigate if and when any of the affected information is accessed by malicious actors.[309] Requiring

[301] For example, as discussed in more detail below, Congress ratified the Commission's 2007 decision to extend section 222-based privacy protections for telecommunications service customers to the customers of interconnected VoIP providers. *See infra* Section III.E.3. And ensuring equivalent protections for TRS subscribers advances Congress' directive to endeavor to ensure functionally equivalent service. *See infra* Section III.E.4.

[302] EPIC et al. Reply Comments at 5-11, 17.

[303] EPIC Comments at 7.

[304] *Pacific Networks Corp. and Comnet (USA) LLC*, Order on Revocation and Termination, FCC 22-22, 37 FCC Rcd 4220, 2022 WL 905270, at *37, para. 82 (Mar. 23, 2022); *China Telecom (Americas) Corporation*, Order on Revocation and Termination, FCC 21-114, 36 FCC Rcd 15966, 16013-14, para. 72 (2021), *aff'd*, *China Telecom (Americas) Corporation v. FCC*, 57 F.4th 256 (D.C. Cir. 2022).

[305] *Data Breach Notice* at 21, para. 42.

[306] 47 CFR § 64.5111(e).

[307] *2007 CPNI Order*, 22 FCC Rcd at 6928, paras. 1-2 & n.1.

[308] *See supra* note 68.

[309] *Data Breach Notice* at 8, para. 12; *2007 CPNI Order*, 22 FCC Rcd at 6944, para. 27.

notification for accidental breaches will encourage TRS providers to adopt stronger data security practices and will help the Commission and law enforcement to better identify and address systemic network vulnerabilities, consistent with our analysis above.[310]

78. The record in this proceeding confirms the need for the Commission to expand the definition of "breach" in section 64.5111 to include inadvertent disclosures.[311] As AARO note in their comments, the Commission must keep pace with evolving threats to consumer privacy, and "adopt measures that can effectively counter increasingly complex and evolving breaches."[312] AARO further agrees with our assessment that an intentionality requirement would lead to legal ambiguity and underreporting.[313] According to AARO and EPIC, the industry will "continue to witness breaches unless companies that operate in this area" are required or incentivized to "make proper investments in their 'staff and procedures to safeguard the consumer data with which they have been entrusted.'"[314] We agree with these commenters that expanding the definition of "breach" in section 64.5111 to include inadvertent access, use, or disclosure of covered data will help provide this incentive.[315]

79. *Good-Faith Exception*. While we expand the definition of "breach" in section 64.5111 to include inadvertent access, use, or disclosure of covered data, consistent with our approach to the carrier data breach rule, we carve out an exception for a good-faith acquisition of covered data by an employee or agent of a TRS provider where such information is not used improperly or further disclosed. No commenters opposed this amendment to our rules for TRS providers.[316] With only a handful of exceptions, the vast majority of state statutes include a similar provision excluding from the definition of "breach" a good-faith acquisition of covered data by an employee or agent of a company where such information is not improperly used or disclosed further,[317] and we see no reason not to include such an

[310] *See supra* Section III.A.

[311] Accessibility Advocacy and Research Organizations Reply at 6 (AARO Reply).

[312] *Id.*

[313] *Id.*

[314] *Id.* at 7 (quoting EPIC Comments at 3); *see also* EPIC et al. Reply at 16.

[315] The only two commenters who opposed expanding the Commission's definition of "breach" in section 64.5111 to include inadvertent disclosures of customer information were Hamilton Relay and Sorenson, and both modified their opposition to state that they only opposed such an expansion *unless* accompanied by the introduction of a harm-based trigger for data breach notification. *See* Hamilton Relay Comments at 5; Sorenson Comments at 2. As we adopt a harm-based trigger for data breach notifications to consumers below, *see infra* Section III.D.3, there is no need to address these two comments further.

[316] We rejected more general criticisms of such a rule above. *See supra* Section III.A.3.

[317] *See, e.g.*, Ala. Code § 8-38-2(1); Alaska Stat. § 45.48.050; Ariz. Rev. Stat. § 18-551(1)(b); Ark. Code § 4-110-103(1)(B); Cal. Civ. Code § 1798.82(g); Colo. Rev. Stat. § 6-1-716(1)(h); Del. Code tit. 6 § 12B-101(1)(a); D.C. Code § 28-3851(1); Fla. Stat. § 501.171(1)(a); Ga. Code § 10-1-911(1); 9 GCA § 48.20(a); Haw. Rev. Stat. § 487N-1; Idaho Stat. § 28-51-104(2); 815 ILCS § 530/5; Ind. Code § 4-1-11-2(b)(1); Iowa Code § 715C.1(1); Kan. Stat. § 50-7a01(h); KRS § 365.732(1)(a); La. Rev. Stat. § 51.3073(2); Me. Rev. Stat. tit. 10 § 1347(1); Md. Code Com. Law § 14-3504(a)(2); Mass. Gen. Laws § 93H-1(a); Mich. Comp. Laws § 445.63(b); Minn. Stat. § 325E.61 Subd. 1(d); Mo. Rev. Stat. § 407.1500(1)(1); Mont. Code § 30-14-1704(4)(a); Neb. Rev. Stat. § 87-802(1); Nev. Rev. Stat. § 603A.020; N.H. Rev. Stat. § 359-C:19(V); N.J. Stat. § 56:8-161; N.M. Stat. § 57-12C-2(D); N.Y. Gen. Bus. Law § 899-aa(1)(c); N.C. Gen. Stat § 75-61(14); N.D. Cent. Code § 51-30-01(1); Ohio Rev. Code § 1349.19(A)(1)(b)(i); Ohio Rev. Code § 1354.01(C)(1); Okla. Stat. § 74-3113.1(D)(1); Okla. Stat. § 24-162(1); Oregon Rev. Stat. § 646A.602(1); 73 Pa. Stat. § 2302; R.I. Gen. Laws § 11-49.3-3(a)(1); S.C. Code § 39-1-90(D)(1); S.D. Cod. Laws § 20-40-19(1); Tenn. Code § 47-18-2107(a)(1)(B); Tex. Bus. & Com. Code § 521.053(a); Utah Code § 13-44-102(1)(b); 9 V.S.A. § 2430(13)(B); Va. Code § 18.2-186.6(A); V.I. Code tit. 14, § 2209(d); Wash. Rev. Code § 19.255.005(1); W.V. Code § 46A-2A-101(1); Wis. Stat. § 134.98(2)(cm)(2); Wyo. Stat. § 40-12-501(a)(i).

exception in the TRS rule. Our good-faith exception will help reduce overreporting and, by extension, will avoid worrying consumers unnecessarily.

2. Notifying the Commission and Other Federal Law Enforcement of Data Breaches

80. In this section, we require TRS providers to notify the Commission, in addition to the Secret Service and FBI, as soon as practicable, and in no event later than seven business days, after reasonable determination of a breach, except in those instances where a breach implicates fewer than 500 individuals and a TRS provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. Where a breach affects fewer than 500 individuals and the TRS provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, we require that providers report such breaches annually to the Commission, Secret Service, and FBI in a single, consolidated annual filing. We also require TRS providers to report breaches to the Commission, Secret Service, and FBI contemporaneously via the existing centralized portal maintained by the Secret Service, and implement mandatory minimum content requirements for notifications filed with the Commission and law enforcement.

81. *Notification to the Commission and Law Enforcement*. We require TRS providers to notify the Commission, in addition to the Secret Service, and the FBI, of breaches through the central reporting facility. The Commission will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni or a successor URL designated by the Bureau. This requirement is consistent with other federal sector-specific laws, including HIPAA and the Health Breach Notification Rule, which require prompt notification to the Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC), respectively.[318]

82. As the Commission found when it adopted the current data breach rules, notifying law enforcement of breaches is consistent with the goal of protecting customers' personal data because it enables such agencies to investigate the breach, "which could result in legal action against the perpetrators," thus ensuring that they do not continue to breach sensitive customer information.[319] The Commission also anticipated that law enforcement investigations into how breaches occurred would enable law enforcement to advise providers and the Commission to take steps to anticipate and prevent future breaches of a similar nature.[320] While this reasoning remains sound, in the years since our rules were adopted it has become apparent that large-scale security breaches need not be purposeful in order to be harmful. As we discuss above,[321] breaches that occur as a result of lax or inadequate data security practices and employee training can be just as devastating as those perpetrated by malicious actors.[322] Notification to the Commission of breaches, including inadvertent breaches, will provide Commission staff with critical information regarding data security vulnerabilities, and will help to shed light on TRS providers' ongoing compliance with our data breach rules.

83. The record in this proceeding supports requiring TRS providers to notify the Commission, the Secret Service, and the FBI of breaches. EPIC agrees that a breach impacting TRS users requires notification to the Commission in addition to the impacted user(s),[323] and no commenter opposed

[318] 45 CFR § 164.408 ("A covered entity shall, following the discovery of a breach . . . notify the Secretary); 16 CFR § 318.3(a)(2).

[319] *2007 CPNI Order*, 22 FCC Rcd at 6943, para. 27.

[320] *Id.*

[321] *See supra* Section III.A.

[322] *Data Breach Notice* at 13, para. 24.

[323] EPIC et al. Reply at 16.

amending our rules to require notification to the Commission concurrently with the Secret Service and FBI in the specific context of TRS.[324]

84. *Reporting Threshold*. We require providers to inform federal agencies, via the central reporting facility, of all breaches, regardless of the number of customers affected or whether there is a reasonable risk of harm to customers. For breaches that affect 500 or more customers, or for which a TRS provider cannot determine how many customers are affected, we require providers to file individual, per-breach notifications as soon as practicable, but no later than seven business days after reasonable determination of a breach.[325] As we describe below, these notifications must include detailed information regarding the nature of the breach and its impact on affected customers.[326] This same type of notification, and the seven business day timeframe for submission, will also be required in instances where the TRS provider has conclusively determined that a breach affects fewer than 500 customers unless the provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach.

85. For breaches in which a TRS provider can reasonably determine that a breach affecting fewer than 500 customers is not reasonably likely to harm those customers, we require the provider to file an annual summary of such breaches with the Commission, Secret Service, and FBI via the central reporting facility, instead of a notification. TRS providers must submit, via the existing central reporting facility and no later than February 1, a consolidated summary of breaches that occurred over the course of the previous calendar year which affected fewer than 500 customers, and where the provider could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach.[327] In circumstances where a TRS provider initially determines that contemporaneous breach notification to federal agencies is not required under these provisions, but later discovers information that would require such notice, we clarify that a TRS provider must report the breach to federal agencies as soon as practicable, but no later than seven business days after their discovery of this new information.[328] We delegate authority to the Bureau to coordinate with the Secret Service regarding any modification to the portal that may be necessary to permit the filing of this annual summary. We also delegate authority to the Bureau, working in conjunction with the Public Safety and Homeland Security Bureau and the Disability Rights Office, and based on the record of this proceeding—or any additional notice and comment that might be warranted—to determine the content and format requirements of this filing and direct the Bureau to release a public notice announcing these requirements.[329] The first annual report will be due the first February 1 after the Office of Management and Budget (OMB) approves the annual reporting requirement under the Paperwork Reduction Act. The first report should cover all breaches between the effective date of the annual reporting requirement and the remainder of the calendar year.[330]

[324] We rejected more general criticisms of such a rule above. *See supra* Section III.B.1.

[325] *See infra* para. 88.

[326] *See infra* paras. 91-92.

[327] To ensure that TRS providers may be held accountable regarding their determinations of a breach's likelihood of harm and number of affected customers, we require providers to keep records of the bases of those determinations for two years. *See infra*, Appx. A. We also note that TRS providers may voluntarily file notification of such a breach in addition to, but not in place of, this annual summary filing.

[328] *See supra* Section III.B.2.

[329] As above with respect to carriers, we instruct the Bureau to minimize the burdens on TRS providers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. At a minimum, the Bureau should develop requirements that are less burdensome than what is required for individual breach submissions to the reporting facility, and consider streamlined ways for filers to report this summary information. *See supra* Section III.B.3.

[330] *See* CTIA Dec. 6, 2023 *Ex Parte* at 16-17 (asking that the Commission explicitly state the due date of the first annual report and that such report shall cover "events that occur on or after the effective date of the new rules").

86. As we determined above,[331] this reporting threshold will enable the Commission to receive more granular information regarding larger breaches to aid its investigations while also being able to study trends in breach activity through reporting of smaller breaches in annual submissions. Such a reporting threshold is also consistent with many state statutes that require notice of breaches to state law enforcement authorities.[332] Moreover, given our expansion of the definition of "breach" in today's Order to include inadvertent exposure of CPNI and other types of data, allowing TRS providers to file information regarding certain smaller breaches in a summary format on an annual basis will tailor administrative burdens on TRS providers to reflect those scenarios where reporting is most critical.[333] At the same time, requiring TRS providers to report breaches that fall below the threshold in a single, consolidated annual filing will continue to enable the Commission and our federal law enforcement partners to investigate, remediate, and deter smaller breaches.[334] As above, in circumstances where a TRS provider initially determines that contemporaneous breach notification to federal agencies is not required under these provisions, but later discovers information that would require such notice, we clarify that the TRS provider must report the breach to federal agencies as soon as practicable, but no later than within seven business days of their discovery of this new information.[335]

87. We apply this threshold trigger only to notifications to federal agencies, and not to customer notifications. Breaches affecting even just a few customers can pose just as much risk to those customers as could breaches with wider impact. For this reason, as discussed above, we continue to require TRS providers to notify federal agencies within seven business days of breaches that implicate a reasonable risk of customer harm, regardless of the number of customers affected. Doing so will permit federal agencies to investigate smaller breaches where there is a risk of customer harm, and also allow law enforcement agencies to request customer notification delays where such notice would "impede or compromise an ongoing or potential criminal investigation or national security," as specified in our rules.[336]

88. *Timeframe*. We retain our existing rule and require TRS providers to notify the Commission of a reportable breach contemporaneously with the Secret Service and FBI, as soon as practicable, and in no event later than seven business days, after reasonable determination of a breach. While we proposed eliminating the seven business day deadline in the *Data Breach Notice*,[337] the record we received convinces us that we should instead retain the more definite timeframe. We agree with AARO that the earlier TRS users are notified of breaches, the more time they will have to take actions to reduce the extent of the potential damage, and that eliminating the seven business day deadline would potentially extend the period between a breach and notification far beyond the current deadline, thus

[331] *See supra* Section III.B.3.

[332] *See, e.g.*, Cal. Civ. Code § 1798.82(f) (requiring entities to report data breaches affecting 500 residents or more to the state Attorney General); Colo. Rev. Stat. § 6-1-716 (requiring entities to report data breaches affecting 500 residents or more to the state Attorney General); Del. Code tit. 6, § 12B-102(d); Fla. Stat. § 501.171(3)(a); R.I. Gen. Laws § 11-49.3-4(a)(2) (requiring entities to report data breaches affecting 500 residents or more to the state Attorney General and major credit reporting agencies); *see also* 45 CFR § 164.408 (requiring notification to the Secretary of Health and Human Services for breaches of unsecured protected health information involving 500 or more individuals).

[333] *See supra* Section III.B.2.

[334] *Data Breach Notice* at 15, para. 30. We note that no commenter addressed this potential amendment to our rule for TRS providers in response to the *Data Breach Notice*, and we address more general comments in this regard in Section III.B.2, above.

[335] *See supra* Section III.B.2.

[336] *See infra* Appx. A.

[337] *See Data Breach Notice* at 21, para. 42; *id.* at Appx. A.

"leaving consumers unable to remediate harms."[338] We find that retaining the seven business day deadline properly balances the need to afford TRS providers sufficient time to conduct remediation efforts prior to submitting notifications with the need to ensure that customers receive timely notifications regarding breaches affecting their data.[339] There is insufficient evidence that the current timeline is inadequate to accomplish the Commission's goals, and requiring breaches to be reported "as soon as practicable" without a definite timeframe could potentially be interpreted differently by different TRS providers or even by law enforcement and the Commission, thereby placing TRS providers at risk of inadvertently violating the Commission's rules should they construct "as soon as practicable" to mean something different than the Commission.[340]

89. We do not believe it is necessary to shorten the existing timeframe of seven business days. As Sorenson notes, businesses with any Internet presence "must routinely investigate large numbers of potential security events," and find that a shorter deadline would put tremendous pressure on providers to report all potential security incidents before having time to determine whether a breach is reasonably likely to have occurred.[341] Such a result would distract providers from investigating and correcting any incident that may have occurred.[342] As Sorenson notes, the current reporting timeline of seven business days allows providers a reasonable opportunity to investigate potential incidents and determine whether a breach is reasonably likely to have occurred.[343]

90. We disagree with Hamilton Relay that the rigid structure in our current rules is "out of step" with other data breach notification obligations and "does not provide TRS providers with sufficient flexibility to address the different circumstances that surround data breaches."[344] To begin, numerous states as well as HIPAA, the Health Breach Notification Rule, and CIRCIA impose a specific time limit on when breach notifications must be made to the state or relevant federal agency.[345] Furthermore, there is nothing in the record beyond Hamilton Relay's unsupported assertion to indicate that TRS providers find the current seven day business deadline to be unduly burdensome or inflexible. Indeed, Sorenson advocates in favor of retaining the current seven business day deadline.[346] Even if we were to assume the seven business day deadline to be a more burdensome or inflexible standard than a more open-ended standard, we still find that the countervailing interest in ensuring customers are notified quickly of breaches affecting them outweighs this hypothetical burden.[347] As above, we clarify that a reasonable

[338] AARO Reply at 8-9.

[339] *See supra* Section III.B.3.

[340] *See supra* Section III.B.3.

[341] Sorenson Comments at 5.

[342] *Id.*

[343] *Id.*

[344] Hamilton Relay Comments at 7-8.

[345] *See e.g.*, Ala. Code § 8-38-6; Ariz. Rev. Stat. Ann. § 18-552(B); Ark. Code § 4-110-105(b)(2); Colo. Rev. Stat. § 6-1-716(f)(I); Conn. Gen. Stat. § 36a-701b(b)(2)(A); Del. Code tit. 6, § 12B-102(d); Fla. Stat. § 501.171(3)(b); Iowa Code § 715C.2(8); Md. Code Ann., Com. Law § 14-3504(h); N.M. Stat. § 57-12C-10; Or. Rev. Stat. § 646A.604(10); 10 L.P.R.A. § 4052; Tex. Bus. & Com. Code § 521.053(i); 9 V.S.A. § 2435(b)(3)(B)(i); Wash. Rev. Code § 19.255.010(7); 45 CFR § 164.408(c); 16 CFR § 318.4(a); 2242(a)(1)(A). Iowa requires notification within 5 days, HIPAA immediately, and CIRCIA within 72 hours. *See* Iowa Code § 715C.2(8); 45 CFR § 164.408(c); 2242(a)(1)(A); *see also* EPIC Comments at 11 (noting that, "in several states, entities are required to report incidents to the attorney general within three days") (citing Nat'l Conf. of State Legislatures, *Security Breach Notification Laws* (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx).

[346] Sorenson Comments at 5.

[347] *See supra* Section III.B.3.

determination that a breach has occurred does not mean reaching a conclusion regarding every fact surrounding a data security incident that may constitute a breach.[348] Rather, a TRS provider will be treated as having "reasonabl[y] determin[ed]" that a breach has occurred when the provider has information indicating that it is more likely than not that there was a breach.[349]

91. *Content of Notification*. As currently structured, the existing central reporting facility requires TRS providers to report: information relevant to a breach, including TRS provider address and contact information; a description of the breach incident; the method of compromise; the date range of the incident and approximate number of customers affected; an estimate of the financial loss to providers and customers, if any; and the types of data breached.[350] The record supports the imposition of minimum content requirements for breach notifications to the Commission, Secret Service, and FBI.[351]

92. While we find that these existing content requirements are largely sufficient, we agree with AARO that the nature of TRS and the sensitive information involved warrants more granular clarification regarding the required disclosures as part of notifications in that context.[352] As AARO notes, TRS users face privacy risks that voice telephone service users do not face because TRS providers and their commercial partners collect particularly sensitive data about TRS users that could be accessed in a data breach.[353] In particular, TRS providers and their partners have direct access to call audio, transcripts, and other data on the contents of TRS users' conversations.[354] Given this, we find that providers must include a description of the customer information that was used, disclosed, or accessed as part of their notification, including whether data on the contents of conversations, such as call transcripts, are compromised as part of a breach.[355] We note that the actual call audio or transcripts themselves *should not* be disclosed as part of the notification, as doing so would be a violation of the Commission's rules.[356] Because of the unique nature of TRS technology, which often result in the creation of transcripts or similar artifacts, we find that clarifying these additional details of the disclosures will better protect consumers and better enable the Commission and our federal law enforcement partners to investigate, remediate, and deter breaches.

93. *Method of Notification*. Under our current rules, TRS providers are required to notify the Secret Service and FBI "through a central reporting facility" to which the Commission maintains a link on its website.[357] We retain this requirement and revise it slightly to clarify that notifications filed through the existing central reporting facility will be transmitted to and accessible by the Disability Rights Office (DRO) of the Commission's Consumer and Governmental Affairs Bureau (CGB), in addition to the Secret Service and FBI. We delegate authority to the Bureau, working in conjunction with CGB, to ensure that the central reporting facility sufficiently relays notifications to DRO. We find that retaining the existing central reporting facility, rather than creating and operating a new centralized reporting

[348] *See supra* Section III.B.3.

[349] *See supra* Section III.B.3.

[350] *Data Breach Notice* at 13-14, para. 27.

[351] *See* AARO Comments at 6; EPIC Comments at 10-11; AARO Reply at 1-3. Of the commenters who addressed this issue, only Hamilton Relay opposes minimum content requirements for TRS providers, and as their comments pertain specifically to the content of breach notifications to *customers*, we address them below. *See infra* Section III.D.3.

[352] AARO Comments at 5-6.

[353] *Id.* at 1.

[354] *Id.* at 1-2.

[355] *Id.* at 6.

[356] 47 CFR § 64.604(a)(2)(i).

[357] *Id.* § 64.5111(b).

facility as contemplated in the *Data Breach Notice*,[358] will be the simplest and most efficient approach, and will not result in the unnecessary expenditure of resources needed to build and operate a new electronic reporting facility when one already exists. It will also reduce potential provider confusion and simplify regulatory compliance by allowing providers to continue filing notifications through the existing reporting facility.[359]

3. Customer Notification

94. In this section, we introduce a harm-based trigger and eliminate the requirement to notify customers of a breach in any instance where a TRS provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. We also eliminate the mandatory seven business day waiting period to notify customers and instead require TRS providers to notify customers of breaches without unreasonable delay after notification to the Commission and law enforcement, and in no case later than 30 days after reasonable determination of the breach, unless law enforcement requests a longer delay. We recommend minimum categories for information inclusion in customer notifications. We decline to specify the method that notifications to customers must take, instead leaving such a determination to the discretion of TRS providers, except that such notifications must be accessible to TRS users.

95. *Harm-Based Notification Trigger*. Our current TRS data breach rule requires notification to customers in every instance where a breach of their information has occurred, regardless of the risk of harm.[360] We modify that standard and forego the requirement to notify customers of a breach in those instances where a TRS provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. In order to ensure the functional equivalency of TRS, and to ensure that TRS users enjoy the same protections as customers of telecommunications carriers and interconnected VoIP providers, we adopt here the same definition of "harm" as that adopted above in the context of telecommunications carriers, for the reasons stated above.[361]

96. In determining whether "harm" is likely to occur, providers should consider all the factors enumerated in our discussion above.[362] In situations where call content—including call audio, transcripts, or other data on the contents of TRS users' conversations—has been or has the potential to be disclosed as a result of a breach, a TRS provider must assume that harm has or is reasonably likely to occur, and the obligation to notify customers of a breach would remain. As with the rules we adopt for telecommunications services above, where a TRS provider is unable to make a determination regarding harm, the obligation to notify customers of a breach would remain.[363] For the reasons discussed above, and in order to ensure functional equivalency for TRS users, we also adopt a safe harbor under which customer notification is not required where a breach solely involves encrypted data and the TRS provider has definitive evidence that the encryption key was not also accessed, used, or disclosed.[364] To the extent

[358] *Data Breach Notice* at 13, para. 25.

[359] We note that no commenter addressed this potential amendment to our rule governing TRS providers in response to the *Data Breach Notice*, and we discuss more general comments regarding the method of disclosure to the Commission in Section III.B.5, above.

[360] 47 CFR § 64.5111(c), (e).

[361] *See supra* para. 55.

[362] *See supra* Section III.C.1 (enumerating the factors providers should consider when assessing the likelihood of harm to customers, including the sensitivity of the information (including in totality) which was breached, the nature and duration of the breach, mitigations, and intentionality).

[363] *See supra* Section III.C.1.

[364] *See supra* para. 58; *see infra* Appx. A.

that a threat actor appears to have circumvented encryption, however, the TRS provider should conduct a harm-based analysis as if the data was never encrypted.

97. We find that introducing a harm-based trigger for notifications to customers of TRS data breaches will benefit customers by avoiding confusion and "notice fatigue" with respect to breaches that are unlikely to cause harm. Given that it is not only emotionally distressing, but also time consuming and expensive to deal with the fallout of a data breach, we believe that introducing a harm-based trigger will spare customers the time, effort, and financial strain of changing their passwords, purchasing fraud alerts or credit monitoring, and freezing their credit in the wake of any breach that is not reasonably likely to result in harm. A harm-based notification trigger also has a basis in the data breach notification frameworks employed by states, many of which do not require covered entities to notify customers of breaches when a determination has been made that the breach is unlikely to cause harm.[365]

98. We find further that employing a harm-based notification trigger will not only benefit customers, but also assist TRS providers by allowing them to better focus their resources on improving data security and ameliorating the harms caused by data breaches rather than providing notifications to customers in instances where harm is unlikely to occur. Nor will the introduction of a harm-based trigger overburden providers by saddling them with the task of determining whether particular breaches are reasonably likely to cause harm. By making the standard for notification a rebuttable presumption of harm, providers must assume that harm is reasonably likely to occur as a result of a breach except where they can reasonably determine otherwise.

99. When determining whether a breach is reasonably likely to result in harm, TRS providers should consider the same factors laid out in our discussion above.[366] In addition, in situations where call content—including call audio, transcripts, or other data on the contents of TRS users' conversations—has been or has the potential to be disclosed as a result of a breach, a TRS provider must assume that harm has or is reasonably likely to occur, and the obligation to notify customers of a breach would remain. TRS providers must construe "harm" in this context broadly.[367] Even in those instances where no harm to customers is reasonably likely to occur, and thus the requirement to notify customers of a data breach is not triggered, TRS providers must still notify the Commission, Secret Service, and FBI of any such breach affecting 500 or more customers as soon as practicable and in any event no later than seven business days after reasonable determination of the breach via the central reporting facility. In the case of such breaches affecting fewer than 500 customers, they must be reported annually in a single, consolidated filing to the Commission, Secret Service, and FBI. While a harm-based trigger will help

[365] *See, e.g.*, Alaska Stat. § 45.48.010(c); Ariz. Rev. Stat. § 18-552(J); Conn. Gen. Stat. § 36a-701b(b)(1) (exempting entities from disclosing breaches when an investigation determines that no harm is likely); Ark. Code § 4-110-105(d) (stating that notice is not required if there is no reasonable likelihood of harm); Fla. Stat. § 501.171(4)(c) (stating that no notice is required if it is reasonably determined that breach has not and will not likely result in identity theft or any other financial harm); Iowa Code § 715C.2(6) (stating that no notice is required if no reasonable likelihood of financial harm has resulted or will result from the breach); Or. Rev. Stat. § 646A.604(8) (stating that no notice is required if no reasonable likelihood of harm has resulted or will result from the breach); N.J. Stat. Ann. § 56:8-163(a) (stating that notice is not required if it is determined that misuse of the information is not reasonably possible); 9 V.S.A. § 2435(d)(1); Md. Com. Law Code Ann. § 14-3504(b); *see also* OMB M-17-12, at 29 (granting federal agencies discretion on whether to notify individuals potentially affected by a breach when the assessed risk of harm is low, and advising agencies to "balance the need for transparency with concerns about over-notifying individuals").

[366] *See supra* Section III.C.1 (enumerating the factors providers should consider when assessing the likelihood of harm to customers, including the sensitivity of the information (including in totality) which was breached, the nature and duration of the breach, mitigations, and intentionality).

[367] *See* AARO Reply at 5 ("[B]ecause TRS involves such sensitive data, a breach that does not create financial or tangible harm may still cause dignitary harm to a TRS user. In that case, such a user has the right to notification. TRS users have no choice but to hand over extremely sensitive information to TRS providers. They should be empowered to know when that data is breached.").

reduce customer notice fatigue and spare customers the time, effort, and financial strain of dealing with the fallout of a breach that is not reasonably likely to result in harm, the Commission and our law enforcement partners can still garner critical information regarding data security vulnerabilities by analyzing larger breaches, even those that are not reasonably likely to result in harm to customers.

100. The record generally supports the adoption of a harm-based trigger for TRS consumer breach notifications.[368] AARO, however, argues that "harm-based triggers should not be used in the context of TRS breach reporting to customers . . . because of the inherent privacy risks faced by TRS users."[369] AARO goes on to argue that, because TRS involves the collection of data on the content of a user's conversation, the Commission should presume that any data breach of a TRS provider is harmful and require the disclosure of that breach to customers and law enforcement.[370] While we agree that the Commission and law enforcement should be apprised of all breaches, we disagree that customers must be made aware of breaches where no harm to customers is reasonably likely to result. While we agree that TRS users face heightened privacy risks because of the nature of the technology involved, such risk alone does not justify a requirement that customers receive notification of breaches in instances where a provider can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach. TRS providers can and *must* take the heightened risks inherent to TRS users into account when determining whether harm is likely to result in the wake of a breach, and we reiterate that providers must assume, in every case, that harm is reasonably likely to occur as a result of a breach *except* where they can reasonably determine otherwise. Moreover, we reiterate that, in situations where call content—including call audio, transcripts, or other data on the contents of TRS users' conversations—has been or has the potential to be disclosed as a result of a breach, a TRS provider must assume that harm has or is reasonably likely to occur, and the obligation to notify customers of a breach would remain. We agree with AARO that, given the sensitive data at stake, "it is conceivable that a TRS user would want to be aware of a data breach, even if the harm of that breach is not fully determined, so that they can take remedial measures," which is why we impose a rebuttable presumption of harm that requires notification in cases where the harm of a breach cannot be fully determined, or where call content has been or has the potential to be disclosed.[371] We find that imposing a rebuttable presumption of harm, and requiring TRS providers to consider the heightened privacy risks experienced by TRS users when attempting to rebut this presumption, sufficiently addresses AARO's concerns without the need for mandatory consumer notifications that may result in notice fatigue and obligate consumers to expend time, effort, and resources dealing with the fallout of breaches that are not reasonably likely to result in harm.

101. We agree with Sorenson that, without a harm-based trigger, our rules could result in over-notification regarding non-critical security events without any corresponding benefit to consumers.[372] We also agree with Hamilton Relay that such over-notification could very well result in notice fatigue and consumer indifference,[373] which would perversely cause consumers to ignore or discount notifications, leading to failure to take action even in those instances where a breach is substantially likely to result in harm, and thus eliminating the main benefit of requiring consumer notifications. We therefore conclude that a harm-based trigger strikes the correct balance between keeping TRS users adequately informed, and reducing over-notification and notice fatigue while reducing the attendant burdens on TRS providers.

102. We disagree with EPIC that a harm-based trigger will lead to "legal ambiguity and underreporting," or that it will delay reporting "as it may take time to assess whether the minimum

[368] *See* Hamilton Relay Comments at 6-7; Sorenson Comments at 2-3; Convo Communications Reply at 8.

[369] AARO Comments at 5; *see also* AARO Reply at 3-4.

[370] AARO Comments at 5; *see also* EPIC et al. Reply at 16.

[371] *See* AARO Reply at 5; *see also infra* Appx. A, § 64.5111(b).

[372] Sorenson Comments at 2-3; *see also* Convo Communications Reply at 8.

[373] Hamilton Relay Comments at 6-7.

threshold for reportable harm has been met."[374] By adopting a rebuttable presumption of harm and requiring consumer notification except in those instances where a provider can reasonably determine that no harm to customers is reasonably likely to occur, we do not think that underreporting is a likely risk, as customers will still be made aware of breaches where protective action from the consumer is required. While we do not here include a specific definition of how or under what circumstances this presumption may be rebutted—finding that such an approach would be too prescriptive—we nevertheless provide guidance for evaluating customer harm, as outlined above.[375] And, as discussed below, we require notification to customers without unreasonable delay after notification to law enforcement, and in no case later than 30 days after reasonable determination of a breach unless law enforcement requests a longer delay.[376]

103. *Notifying Customers of Data Breaches Without Unreasonable Delay*. Our current TRS data breach rule prohibits TRS providers from notifying customers or disclosing a breach to the public until at least seven full business days after notification to the Secret Service and FBI.[377] We eliminate this mandatory waiting period and instead require TRS providers to notify customers of CPNI breaches without unreasonable delay after notification to law enforcement, and in no case later than 30 days after reasonable determination of a breach, unless law enforcement requests a longer delay.

104. In adopting the current rule, the Commission concluded that once customers have been notified of a breach, it becomes public knowledge, "thereby impeding law enforcement's ability to investigate the breach, identify the perpetrators, and determine how the breach occurred."[378] The Commission found that "immediate customer notification may compromise all the benefits of requiring carriers to notify law enforcement of CPNI breaches," and that a short delay was thus warranted.[379]

105. As discussed above,[380] given the sheer volume of personal data at risk, and the proliferation of malicious schemes designed to exploit that data, we find that the need to notify victims of breaches as soon as possible has grown exponentially in the years since our rules were adopted. The rules we adopt in this Order will better serve the public interest by increasing the speed at which customers may receive the important information contained in a notification, except in those circumstances when law enforcement specifically requests otherwise.[381] We find that a requirement to notify customers of data breaches without unreasonable delay after discovery of a breach and notification to law enforcement appropriately balances legitimate law enforcement needs with customers' need to take swift action to protect their information in the wake of a breach.

[374] EPIC Comments at 8; *see also* AARO Reply at 4.

[375] *See supra* Section III.C (enumerating the factors providers should consider when assessing the likelihood of harm to customers, including the sensitivity of the information (including in totality) which was breached, the nature and duration of the breach, mitigations, and intentionality).

[376] *See infra* para. 103.

[377] 47 CFR § 64.5111(b)(1).

[378] *2007 CPNI Order*, 22 FCC Rcd at 6943-44, para. 28.

[379] *Id.* at 6944, para. 28.

[380] *See supra* Section III.C.2.

[381] *Cf., e.g.*, R.I. Gen. Laws § 11-49.3-4(a)(2), (b) (requiring notification to state Attorney General and major credit reporting agencies if more than 500 residents are affected by a breach, specifying that such notice should be made *without* delaying notice to affected residents, and permitting law enforcement to delay notification if necessary for investigation).

106. Our revised rule is consistent with many existing data breach notification laws that require expedited notice but refrain from requiring a specific timeframe.[382] While requiring notification to customers without unreasonable delay will increase the speed at which customers receive important information related to a breach, we decline to adopt a specific timeframe, and find that such an approach would be overly prescriptive. Because each data breach is different, providers must be given sufficient latitude to address each breach separately, in the manner best befitting the nature of the breach. Even so, we find it appropriate to impose an outside limit on when customers must be notified of a breach. Requiring providers to notify customers no later than 30 days after reasonable determination of a breach, unless a longer delay is requested by law enforcement, will allow TRS providers sufficient flexibility to deal with each breach on an individual basis while simultaneously installing a backstop to ensure that customers are not made unaware of a breach indefinitely.

107. This approach is generally consistent with HIPAA, which requires notification to individuals "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach,"[383] as well as the Health Breach Notification Rule, which requires notification to individuals "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security."[384] Additionally, many states impose an outside limit on when customers must be notified of a breach following discovery of said breach.[385]

108. Consistent with our current rules implementing section 222, the rule we adopt today will allow law enforcement to direct a TRS provider to delay customer notification for an initial period of up to 30 days if such notification would interfere with a criminal investigation or national security.[386] We find that in those instances where a provider reasonably decides to consult with law enforcement, a short initial delay of no longer than 30 days pending such consultation is reasonable under the "without unreasonable delay" standard we adopt for customer notification. We note that HIPAA, the GLBA, and the Health Breach Notification Rule all allow for a delay of customer notification if law enforcement determines notification to customers would "impede a criminal investigation or cause damage to national security," but only if law enforcement officials request such a delay.[387] More specifically, both HIPAA and the Health Breach Notification Rule allow for notification delays of up to 30 days if orally requested

[382] *See, e.g.*, 12 CFR pt. 364, Appx. B, Supp. A § III(A)(1) (interpreting GLBA § 501(b)) (requiring customer notification "as soon as possible" after a determination that customer information has been misused or misuse is reasonably possible); Cal. Civ. Code § 1798.82(a) (requiring notification to "be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement"); Va. Code Ann. § 18.2-186.6(B) ("without unreasonable delay"); D.C. Code § 28-3852(a) ("in the most expedient time possible and without unreasonable delay"); Wyo. Stat. Ann. § 40-12-502(a) ("notice shall be made in the most expedient time possible and without unreasonable delay"); *see also* FTC Data Breach Guide at 6 (explaining that, "if you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused").

[383] 45 CFR § 164.404(b). For breaches involving more than 500 residents of a state or other jurisdiction, HIPAA also requires notification of "prominent media outlets serving the State or Jurisdiction" without unreasonable delay and no later than 60 calendar days after discovery of a breach. *Id.* § 164.406. For breaches involving 500 or more residents of a state or other jurisdictions, HIPAA also requires notification to the Secretary of Health and Human Services (HHS). *Id.* § 164.408.

[384] 16 CFR § 318.4(a).

[385] *See, e.g.*, Ala. Code § 8-38-5(b); Ariz. Rev. Stat. Ann. § 18-552(B); Colo. Rev. Stat. § 6-1-716; Del. Code Ann. Tit. 6, § 12B-102(c); Fla. Stat. § 501.171(4)(a); Md. Code Ann. § 14-3504(b)(3); N.M. Stat. Ann. § 57-12C-6(A); Ohio Rev. Code Ann. § 1349.19(B)(2); Or. Rev. Stat. § 646A.604(3)(a); R.I. Gen. Laws § 11-49.3-4(a)(2); S.D. Codified Laws § 22-40-20; Tenn. Code § 47-18-2107(b); Vt. Stat. Ann. Tit. 9, § 2435(b)(1); Wash. Rev. Code § 19.255.010(8).

[386] 47 CFR § 64.5111(b)(3).

[387] *See* 16 CFR § 318.4(c); 12 CFR part 364, Appx. B, Supp. A; 45 CFR § 164.412.

by law enforcement.[388] Similarly, most, if not all, states permit delays in notifying affected customers for legitimate law enforcement reasons.[389] We find that the rule we adopt today strikes the appropriate balance between the needs of law enforcement to have sufficient time to investigate criminal activity and the needs of customers to be notified of data breaches without unreasonable delay.

109. The record supports reconfiguring our rules in this manner. As Hamilton Relay notes, TRS providers require flexibility when addressing data breaches,[390] and a standard requiring providers to notify customers of a breach as soon as practicable will allow TRS providers sufficient time to determine the nature of the incident, "including what consumer data may be implicated, if any.[391] And we agree with Sorenson that imposing a rigid timeline on providers without offering sufficient time to investigate runs the risk of placing "tremendous pressure on providers to report all potential security incidents before having time to determine whether a breach is reasonably likely to have occurred," and that such a result would not only overload the Commission but "also distract providers from investigating and correcting any incident that may have occurred."[392] We find that retaining our seven business day deadline for federal-agency notifications will allow TRS providers a reasonable opportunity to investigate potential incidents, determine whether a breach is reasonably likely to have occurred, and report it to the Commission and our law enforcement partners, if necessary,[393] while the elimination of the mandatory seven business day waiting period and imposition of a 30-day backstop will ensure that customers receive notification of any such breach in a timely fashion.

110. We disagree with AARO that the timeframe revisions we make will result in unwarranted delays of notifications to customers.[394] On the contrary, we find that our pairing of an unreasonable delay standard with our elimination of the mandatory seven business day waiting period between notification of law enforcement and notification of customers is more likely to result in consumers receiving notice of a breach more quickly than they would under our current rule in many instances. By requiring TRS providers to issue consumer notifications without unreasonable delay, but in no case later than 30 days after a breach has been detected unless a longer delay is requested by law enforcement, we believe that our revised rule balances the needs of law enforcement and TRS providers—to respond flexibly, with sufficient time to investigate data breaches—and customers—to take swift action in the wake of a breach.

111. *Content of Customer Breach Notification*. Consistent with our current TRS data breach rule, we decline to adopt specific minimum categories of information required in a customer breach notification.[395] We make clear, however, that a notification must include sufficient information so as to

[388] 45 CFR § 164.412; 16 CFR § 318.4(c); *see also* 12 CFR part 364, Appx. B, Supp. A § III(A)(1) (allowing that "customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for a delay").

[389] *See, e.g.*, Alaska Stat. Ann. § 45.48.020 ("An information collector may delay disclosing the breach . . . if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation."); Ariz. Rev. Stat. Ann. § 18-552(D) ("The notifications required by subsection B of this section may be delayed if a law enforcement agency advises the person that the notifications will impede a criminal investigation."); Cal. Civ. Code § 1798.82(c) ("The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation."); Conn. Gen. Stat. Ann. § 36a-701b(d) ("Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed.").

[390] Hamilton Relay Comments at 7.

[391] *Id.* at 8-9; *see also* Convo Communications Reply at 8-9.

[392] Sorenson Comments at 5.

[393] *Id.*

[394] AARO Reply at 8-9.

[395] 47 CFR § 64.5111.

make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. While all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have laws requiring private or governmental entities to notify individuals of breaches involving their personal information,[396] of these, less than half impose minimum content requirements on the notifications that must be transmitted to affected individuals in the wake of a data breach.[397] As noted above regarding carriers, adding requirements with the potential to differ from such a high number of state requirements may create unnecessary burdens on small TRS providers.[398] We also find that specifying the required content of customer notifications beyond the basic standard described above would inhibit TRS providers from having the flexibility to craft notifications that are more responsive to, and appropriate for, the specific facts of a breach, the customers, and the provider involved. A stricter standard could conflict with other customer notice requirements—thus burdening providers and potentially sowing confusion among consumers—and could delay providers' ability to timely notify their customers of a breach, since it could take time to gather all of the necessary details and information even in cases where it would be in customers' best interests to receive notification more quickly, albeit with less detail.[399]

112. Instead, we adopt as recommendations the following categories of information in security breach notifications to TRS customers: (1) the date of the breach; (2) a description of the customer information that was used, disclosed, or accessed; (3) whether data on the contents of conversations, such as call transcripts, was compromised as part of the breach;[400] (4) information on how customers can contact the provider to inquire about the breach; (5) information about how to contact the Commission, FTC, and any state regulatory agencies relevant to the customer and the service; (6) if the breach creates a risk of identity theft,[401] information about national credit reporting agencies and the steps customers can take to guard against identity theft, including any credit monitoring, credit reporting, or credit freezes the

[396] *See* Nat'l Conf. of State Legislatures, *Security Breach Notification Laws* (Jan. 17, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[397] *See, e.g.*, Ala. Code § 8-38-5(d); Ariz. Rev. Stat. § 18-552(E); Cal. Civ. Code § 1798.82(d)(2); Colo. Rev. Stat. § 6-1-716(2)(a.2); 815 ILCS § 530/10(a)(1); Md. Code Com. Law § 14-3504(g), Md. State Govt. Code § 10-1305(g); Mass. Gen. Laws ch. 93H-1, § 3(b); Mich. Comp. Laws § 445.72(6)(c)-(g); N.Y. Gen. Bus. Law § 899-AA(7); Oregon Rev. Stat. § 646A.604(5); 9 V.S.A. § 2435(b)(5); Wash. Rev. Code §§ 19.255.010(6)(b), 42.56.590(6)(b); *see also* 45 CFR § 164.404(c)(1); Am. Bankers Ass'n, *Data Security & Customer Notification Requirements for Banks*, https://www.aba.com/banking-topics/technology/data-security/data-security-customer-notification; *Final Guidance on Response Programs: Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, Federal Deposit Insurance Corporation, Michael J. Zamorski, Director, Division of Supervision and Consumer Protection, Financial Institution Letters, FIL-27-2005 (Apr. 1, 2005), https://www.fdic.gov/news/financial-institution-letters/2005/fil2705.html (*GLBA Customer Notice Guidance*); FTC Data Breach Guide.

[398] *See supra* Section III.C.3.

[399] *See supra* Section III.C.3.

[400] AARO Comments at 6.

[401] Breaches which involve data such as a social security number, birth certificate, taxpayer identification number, bank account number, driver's license number, and other similar types of personally identifiable information unique to each person create the highest level of risk of identity theft. *See* Am. Bar Ass'n, *Identity Theft and Fraud: How to Evaluate and Manage Risks* (Mar. 2020), https://www.americanbar.org/news/abanews/publications/youraba/2020/youraba-march-2020/identity-theft-and-fraud. While breaches involving the types of data listed here should be considered to create a risk of identity theft for customers, this is not an exclusive list and should not be considered as such. There may be other types of data not listed here that, either alone or in conjunction with other data, may potentially create a risk of identity theft for customers.

provider is offering to affected customers; and (7) what other steps customers should take to mitigate their risk based on the specific categories of information exposed in the breach.

113. We find that adopting recommendations for minimum consistent fields of information will further the goal of assisting customers in better understanding the circumstances and nature of a breach while retaining some flexibility for TRS providers to precisely tailor each notification, depending on the specific facts and details of each breach.[402] We agree with Hamilton Relay that the Commission should give providers the flexibility to craft breach notifications that include relevant information in an accessible format,[403] depending on the circumstances of each breach. While we acknowledge arguments by AARO and EPIC supporting the imposition of minimum content requirements for customer breach notifications,[404] we are wary of imposing specific requirements that could conflict with many state regulations, and of attempting to impose a one-size-fits-all solution for all providers and all data breaches. Rather, we find that the seven categories of information we recommend appropriately balance our goal of empowering consumers to take the necessary steps to protect themselves and their information in the wake of a data breach while simultaneously enabling TRS providers to respond flexibly to data breaches as they occur, and to issue customer notifications as swiftly as possible without the need to delay as they gather all of the information needed to satisfy a rigidly prescribed set of predetermined informational categories.

114. *Method of Customer Breach Notification*. We decline to specify the form that notifications to customers must take, instead leaving such a determination to the discretion of TRS providers, except to require that such notifications be provided in a format accessible to individuals with disabilities. In this proceeding, commenters were uniform in their insistence that the method of customer breach notification be left to the discretion of providers where it is not specified in state law.[405] As CCA notes, the "best means for reaching business customers and residential customers . . . can differ significantly, and carriers are best positioned based on their experience and contact with consumers to know customers' preferred way of receiving notifications."[406] CTIA argues further that mandating the manner of customer CPNI incident notifications could "reduc[e] carrier flexibility to provide the most up-to-date information to customers in fluid situations."[407] As Hamilton Relay points out, "TRS providers do not have standard billing information for their customers because . . . most if not all TRS users do not pay for the service."[408] Because this lack of standard billing information may complicate notifications to such users, we agree with Hamilton Relay that the Commission should grant TRS providers the discretion to take all reasonable steps necessary to provide the required information to their customers in a "usable and readily understandable format" whenever a breach occurs.[409] We thus decline to specify the manner that accessible notifications to customers must take, and leave such a determination to the discretion of TRS providers where the manner of customer breach notifications is not specified by applicable state law.

115. *TRS User Registration Information*. In their comments, Sorenson notes that "TRS customers must undergo intrusive identity and address verification that other voice telephone customers

[402] *See supra* Section III.C.3.

[403] Hamilton Relay Comments at 3-4.

[404] AARO Comments at 5-6; EPIC Comments at 8, 10-11; AARO Reply at 1-2.

[405] *See* Blooston Rural Carriers Comments at 6; CCA Comments at 8; CTIA Comments at 31-32; USTelecom Comments at 2, 8; CTIA Reply at 24.

[406] CCA Comments at 8.

[407] CTIA Comments at 32.

[408] Hamilton Relay Comments at 4-5.

[409] *Id.* at 5.

do not,"[410] and that data retention requirements of TRS providers put customers who rely on these critical services at heightened risk.[411] Sorenson thus recommends that our revised rules permit TRS providers to delete sensitive customer information, such as copies of users' driver's licenses/passports and other identity or address identifying information.[412] Convo Communications take this recommendation a step further, advocating that the Commission not just permit but *require* providers to destroy identifying records regarding TRS users after a user is successfully registered in the TRS User Registration Database (TRS URD).[413]

116. We decline to adopt these recommendations at this time. The requirements to collect and retain user registration information for registration in the TRS User Registration Database are outside the scope of this proceeding. The TRS User Registration Database is a centralized system of registration records established to protect the TRS Fund from waste, fraud, and abuse and to improve the Commission's ability to manage and oversee the TRS program.[414] A necessary component of the administration and oversight of the TRS User Registration Database and the TRS program in general, is the ability of the Commission, the TRS User Registration Database administrator, and the TRS Fund administrator to review and audit the registration information of TRS users and the registration practices of TRS providers. Any consideration of changes to the rules concerning TRS providers retaining required registration information for TRS users must include an assessment of the impact of the ability of the Commission and relevant administrators to review the data upon which users were verified in the database. The record in this proceeding is incomplete as the Commission did not seek comment on this issue. We therefore do not take action on this issue at this time.

E. Legal Authority

117. We find that sections 201(b), 222, 225, and 251(e) provide us with authority to adopt the breach notification rules enumerated in this Order. We conclude further that we have authority to apply these revised rules to interconnected VoIP providers. Lastly, we find that Congress' nullification of the Commission's revisions to its data breach rules in the *2016 Privacy Order* pursuant to the Congressional Review Act (CRA) does not now preclude us from adopting the rules set forth in this Order.[415]

1. Section 222

118. Section 222 of the Act provides authority for the requirements we adopt and revise today.[416] Section 222(a) imposes a duty on carriers to "protect the confidentiality of proprietary

[410] Sorenson Comments at 6.

[411] *Id.* at 6-8.

[412] *Id.* at 8.

[413] Convo Communications Reply at 4-7; *see also* AARO Reply at 10.

[414] 47 CFR § 64.601(a)(48); *id.* § 64.611(a), (j).

[415] *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, 31 FCC Rcd 13911, 14019-33, paras. 261-91 (2016) (*2016 Privacy Order*); Resolution of Disapproval ("*Resolved by the Senate and House of Representatives of the United States of America in Congress assembled,* That Congress disapproves the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016)), and such rule shall have no force or effect."); 5 U.S.C. § 801(f) ("Any rule that takes effect and later is made of no force or effect by enactment of a joint resolution under section 802 shall be treated as though such rule had never taken effect."); 5 U.S.C. § 801(b)(1) ("A rule shall not take effect (or continue), if the Congress enacts a joint resolution of disapproval . . . of the rule."); *see also 2017 CRA Disapproval Implementation Order*.

[416] *See Data Breach Notice* paras. 46-47.

information of, and relating to" customers, fellow carriers, and equipment manufacturers.[417] Section 222(c) imposes more specific requirements on carriers as to the protection and confidentiality of customer proprietary network information.[418] Both subsections independently provide us authority to adopt rules requiring telecommunications carriers and interconnected VoIP providers to address breaches of customer information, but the breadth of section 222(a) provides the additional clarity that the Commission's breach reporting rules can and must apply to all PII rather than just to CPNI.

119. The Commission has long required carriers to report data breaches as part of their duty to protect the confidentiality of customers' information.[419] The revisions to the Commission's data breach reporting rules adopted in this Order reinforce carriers' duty to protect the confidentiality of their customers' information, including information that may not fit the statutory definition of CPNI. Data breach reporting requirements also reinforce the Commission's other rules addressing the protection of customer information by meaningfully informing customer decisions regarding whether to give, withhold, or retract their approval for carriers to use or disclose their information. Moreover, requiring carriers to notify the Commission in the event of a data breach will better enable the Commission to identify and confront systemic network vulnerabilities and help investigate and advise carriers on how best to avoid future breaches, while simultaneously assisting carriers in fulfilling their duty pursuant to section 222(a) to protect the confidentiality of their customers' information.[420]

120. We reject Lincoln Network's argument that section 222 does not grant us authority to adopt rules requiring telecommunications carriers and interconnected VoIP providers to address breaches of covered data.[421] Section 222 explicitly imposes a duty on telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers."[422] To argue, as Lincoln Network does, that section 222 does not grant the Commission "clear authority to protect the security of data"[423] contravenes the clear language and intent of section 222.[424] Ever since it began implementation of the 1996 Act, the Commission has understood section 222(a) as a source of carriers' duties and as a source of Commission rulemaking authority.[425] To the extent that the Commission has described its section 222 authority as coextensive with the definition of CPNI, we disavow such an interpretation. In those proceedings, the Commission was not examining the distinction between CPNI and other sensitive personal information, and it never explicitly decided that section 222(a) does not reach other forms of personal information. In fact, the Commission in 2007 described section 222(a)'s duty as extending to "proprietary or personal customer information,"[426] and more recent enforcement actions have affirmed that carriers' duty to protect customer information extends

[417] 47 U.S.C. § 222(a); *see* H.R. Rep. No. 104-458 at 205 ("New subsection 222(a) stipulates that it is the duty of every telecommunications carrier to protect the confidentiality of proprietary information of and relating to other carriers, equipment manufacturers and customers . . . .").

[418] 47 U.S.C. § 222(c).

[419] *See 2007 CPNI Order*, 22 FCC Rcd at 6943-45, paras. 26-32.

[420] 47 U.S.C. § 222(a).

[421] *See generally* Lincoln Network Comments.

[422] 47 U.S.C. § 222(a).

[423] Lincoln Network Comments at 1-2.

[424] 47 U.S.C. § 222(a).

[425] *See 1998 CPNI Order*, 13 FCC Rcd at 8196, para. 194 ("[S]ection 222(a) specifically imposes a protection duty . . . ."); *id.* at 8200, para. 203 ("The Commission in the *Notice* focused on issues relating to the implementation of sections 222(c)-(f). Based on various responses from parties, we now seek further comment on three general issues that principally involve carrier duties and obligations established under sections 222(a) and (b) of the Act.").

[426] *2007 CPNI Order*, para. 64.

beyond CPNI.[427] To find that carriers have no duty to protect the confidentiality of non-CPNI PII would be inconsistent with the plain language of section 222(a)'s use of the term "proprietary information of, and relating to, . . . customers" and is not the best interpretation of that provision. Instead, consistent with those recent Commission actions, we find that the phrase "information of, and relating to, . . . customers" in section 222(a) is naturally—and indeed best—interpreted to have the same definition as PII, subject to the additional limitation that the information be "proprietary" to the carrier—i.e., obtained in connection with establishing or maintaining a communications service.[428] Finally, given the larger context discussed below,[429] to the extent that an obligation to take reasonable measures to protect all PII were not derived directly from section 222(a), that would be because Congress understood it already to be based in section 201(b)'s prohibition on unjust or unreasonable practices.

121. Some commenters contend that section 222(a) simply sets out high-level principles the substantive details of which are specified elsewhere.[430] But even beyond our foregoing analysis, that interpretation of section 222(a) is at odds with the fact that section 222(a) lists "equipment manufacturers" among the classes of entities owed confidentiality protections as part of a carrier's "general" duty.[431] Given that section 222 never otherwise mentions confidentiality protections owed to those entities, this reinforces our view that section 222(a) is best read as imposing enforceable obligations on telecommunications carriers separate and apart from the requirements of section 222(b) and (c).[432] Nor

[427] *TerraCom NAL*, 29 FCC Rcd at 13330-32, paras. 14-20. As noted below, the general interpretation of section 222 in the *TerraCom NAL* also was confirmed by the Commission in a subsequent rulemaking order. *See infra* note 442. And as noted above, in November 2021 and March 2022 orders revoking the operating authority of certain telecommunications carriers, the Commission further stated that all communications service providers have "a statutory responsibility to ensure the protection of customer information, including PII and CPNI." *See supra* note 304.

[428] NCTA asserts that "most PII . . . is not 'proprietary information," but does not justify why we should adopt an understanding of that term different than the one here. NCTA Dec. 5, 2023 *Ex Parte* at 2.

[429] *See infra* Section III.E.2 (discussing authority under section 201(b)).

[430] *See, e.g.*, CTIA Comments at 11-12; NCTA Dec. 5, 2023 *Ex Parte* at 4; CTIA Dec. 6, 2023 *Ex Parte* at 2-3. We reject NCTA's claim that "legislative history supports an interpretation of Section 222 that does not impose an affirmative obligation under Section 222(a), which shows that Congress deliberately chose not to use 'personally identifiable information' in Section 222." NCTA Dec. 5, 2023 *Ex Parte* at 4. NCTA cites a statement from the conference report that "'the new section 222 strives to balance both competitive and consumer privacy interests with respect to CPNI.'" NCTA Dec. 5 *Ex Parte* at 4 (quoting H.R. Conf. Rep. No. 104-458, at 205 (Jan. 31, 1996) (Conf. Rep.)). But as even commenters opposed to our interpretation of section 222(a) recognize, section 222 applies to more than just CPNI, undercutting any understanding of that statement as reflecting the full scope and contours of section 222. *See, e.g.*, CTIA Comments at 11 (observing that section 222(b) imposes certain obligations on carriers with respect to the proprietary information of other carriers). NCTA also cites a House Report discussing earlier statutory language considered by the House, which would have specified a different scope of covered information. NCTA Dec. 5 *Ex Parte* at 4 (citing H.R. Rep. No. 104-204, Pt. I, 104th Cong., 1st Sess., at 23 (July 24, 1995) (July 24, 1995 House Rep.)). But that alternative definition also was part of a statutory provision that different in many other ways from section 222 as ultimately adopted, *see* July 24, 1995 House Rep., at 22-23, and section 222 as enacted ultimately was based on the Senate version. Conf. Rep. at 205. In sum, we see nothing in the legislative history that would persuade us to depart from what we see as the best interpretation of section 222(a) based on the statutory text.

[431] 47 U.S.C. § 222(a).

[432] Admittedly, as CTIA points out, *see* CTIA Comments at 12, section 273(d)(2) separately prohibits "[a]ny entity which establishes standards for telecommunications equipment or customer premises equipment, or generic network requirements for such equipment, or certifies telecommunications equipment or customer premises equipment . . . from releasing or otherwise using any proprietary information, designated as such by its owner, in its possession as a result of such activity, for any purpose other than purposes authorized in writing by the owner of such information." 47 U.S.C. § 273(d)(2). But CTIA fails to demonstrate that the entities that are the focus of section 222(a)—i.e., telecommunications carriers—are fully subsumed by (or even substantially overlap with) the entities that are the

(continued….)

does section 222(a) otherwise include textual indicia at odds with our understanding. Section 222(a) employs regulatory terminology in imparting a general "duty" on telecommunications carriers. Section 222(a)'s heading of "In General" also is fully compatible with our understanding of that provision as imposing a general duty—in contrast to alternative headings such as "Purpose" or "Preamble" that would indicate that the "duty" announced by such a provision is merely precatory or a "statement of purpose" with no legal force of its own.

122. Contrary to some commenters' claims,[433] our interpretation of section 222(a) also otherwise is compatible with the remainder of section 222. We read section 222(a) as imposing a broad duty that can and must be read in harmony with the more specific mandates set forth elsewhere in the statute.[434] Provisions such as sections 222(b) and (c) directly impose specific requirements on telecommunications carriers to address concerns that were particularly pressing at the time of section 222's enactment, which continue to control over the more general duty in section 222(a) to the extent of any overlap. Our interpretation of section 222(a) thus preserves the role of each of these provisions within the section 222 framework. And given the more detailed statutory specification of carriers' requirements regarding CPNI in section 222, it is understandable the Congress made a point of establishing express exceptions from those requirements in section 222(d).[435] Part of interpreting section 222(a) in harmony with section 222 as a whole includes interpreting it in harmony with section 222(d). Thus, we do not interpret the grounds for disclosure authorized by section 222(d) as violating carriers' obligation to protect the confidentiality of proprietary information imposed by section 222(a). Our analysis is the same regarding other provisions of section 222, such as the subscriber information disclosure requirements in section 222(e) and (g).[436] Thus, we do not interpret section 222(a) to impose obligations inconsistent with those disclosure requirements, either. Because we read section 222(a) in harmony with the remainder of section 222 there is no incompatibility in our approach. And the mere omission of section 222(a) from provisions like section 222(d), (e), and (g) would have been an oblique and indirect way of dictating an interpretation of section 222(a) that runs counter to its plain meaning: a reasonable person would not interpret "a duty to protect the confidentiality" of customer information as prohibiting its use for billing, for example, as is permitted by section 222(d)(1).

123. Lincoln Network attempts to draw a distinction between security and confidentiality that is unavailing.[437] Lincoln Network itself appears to recognize that something that could be characterized as a "security" breach can result in loss of confidentiality for data or information.[438] Thus, even assuming

(Continued from previous page)
focus of section 273(d)(2)—e.g., entities that establish equipment standards or requirements or certify such equipment. The significant mismatch between sections 222(a) and 273(d)(2) thus gives us no reason to question our understanding of section 222(a).

[433] *See, e.g.*, CTIA Comments at 12-14; NCTA Dec. 5, 2023 *Ex Parte* at 4; CTIA Dec. 6, 2023 *Ex Parte* at 3.

[434] This understanding of section 222(a) also accords with the fact that the Commission generally has relied on a "reasonableness" standard when evaluating carriers' protection of information under section 222. *See, e.g.*, *2007 CPNI Order*, 22 FCC Rcd at 6959, para. 63 (in the event of a breach a carrier "must demonstrate that the steps it has taken to protect CPNI from unauthorized disclosure, including the carrier's policies and procedures, are reasonable" under the circumstances).

[435] 47 U.S.C. § 222(d).

[436] 47 U.S.C. § 222(e), (g).

[437] *See, e.g.*, Lincoln Network Comments at 2-4 (discussing terminology used in certain industry publications); *id*. at 8-9 (citing other federal laws that use both "confidentiality" and "security" or refer to "security" when describing requirements that Lincoln Network sees as analogous to the Commission's data breach reporting requirements).

[438] *See, e.g.*, Lincoln Network Comments at 2 (stating that "[d]ata breaches are cybersecurity attacks that result in the loss of confidentiality of consumer personal information"); *id*. at 4 (citing an industry report as taking the position that "security incidents, . . . may conclude with data breaches"); *id*. (stating that "not all security incidents are data breaches, but all data breaches are security incidents").

arguendo that breaches of security and breaches of confidentiality are not coextensive, that would matter only if the Commission were attempting to act beyond the scope of section 222's statutory grant of authority with respect to confidentiality—which is not the case here. Based on relevant textual indicia, we conclude that "confidentiality" within the meaning of section 222 encompasses impermissible access to, use of, and/or disclosure of covered information.[439] Our data breach reporting requirements focus on "breaches," which occur when "a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data."[440] The "covered data" is defined in terms of the statutory categories of proprietary information and customer proprietary network information, and the focus on access, use, and disclosure of those data fits comfortably within our section 222 authority.

2. Section 201(b)

124. Section 201(b) of the Act requires practices of common carriers to be just and reasonable and declares any unjust or unlawful practices to be unlawful.[441] The Commission concluded in the *TerraCom NAL* that section 201(b) was violated when carriers failed to notify customers whose personal information had been breached by the carriers' inadequate data-security policies.[442] The *TerraCom NAL* explicitly put carriers "on notice that in the future we fully intend to assess forfeitures for such violations" under section 201(b).[443] We therefore conclude that our authority to prohibit unjust and unreasonable practices[444] and to "prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of" the Act pursuant to section 201(b) provides independent authority for us to consider

[439] Section 222(a) establishes carriers' "duty to protect the confidentiality of proprietary information . . . ." 47 U.S.C. § 222(a). Section 222(b), in turn, is entitled "[c]onfidentiality of carrier information," and limits carriers' "use" of proprietary information. 47 U.S.C. § 222(b). Section 222(c) is entitled "[c]onfidentiality of customer proprietary network information" and limits how carriers "use, disclose, or permit access to" individually identifiable CPNI. 47 U.S.C. § 222(c)(1). "Although section headings cannot limit the plain meaning of a statutory text, 'they supply cues' as to what Congress intended." *Merit Management Group v. FTI Consulting*, 138 S. Ct. 883, 893 (2018) (citation omitted). Against that backdrop we reject Lincoln Network's attempts to rely on isolated examples of terminology uses from recent industry reports or the like. *See, e.g.*, Lincoln Network Comments at 2-4.

[440] *See infra* Appx. A, 47 CFR § 64.2011(e)(1); *see also id*., 47 CFR § 64.5111(f)(1).

[441] 47 U.S.C. § 201(b).

[442] *TerraCom NAL*, 29 FCC Rcd at 13329-30, para. 12, 13335-37, paras. 31-35. In a subsequent Report and Order adopting Lifeline rules, the Commission "confirm[ed] the general interpretation of sections 201 and 222 reflected in the *TerraCom NAL*." *Lifeline and Link Up Reform and Modernization et al.*, WC Docket No. 11-42 et al., 30 FCC Rcd. 7818, 7846, para. 65 n.168 (2015).

[443] *TerraCom NAL*, 29 FCC Rcd at 13341, para. 43 n.97; *see* EPIC et al. Reply at 11. As NCTA points out, the Commission did not propose a forfeiture under section 201(b), NCTA Reply at 10-11, but that was because it was the first time the Commission had declared a carrier's practices related to its failure to notify consumers of a data breach to be a violation of section 201(b). The Commission made explicit that, in the future, such violations would be penalized under section 201(b). *TerraCom NAL*, 29 FCC Rcd at 13341, para. 43 n.97 ("Because this is the first time we declare a carrier's practices related to its failure to adequately notify consumers in connection with a security breach unjust and unreasonable in apparent violation of Section 201(b), we do not propose to assess a forfeiture for the apparent violations here. However, through our action today, carriers are now on notice that in the future we fully intend to assess forfeitures for such violations, taking into account the factors identified above."). We now make that clear again here.

[444] *See* EPIC Comments at 7; EPIC et al. Reply at 9-11; *Ambassador, Inc. v. United States*, 325 U.S. 317, 323 (1945) (holding that "the supervisory power of the Commission is not limited to rates and services, but . . . [includes] 'charges, practices, classifications, and regulations for and in connection with such communication service'"); *see also, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, 15233-34, para. 37 (2020).

PII as protected consumer information and to require carriers to notify customers, law enforcement, and the Commission about breaches as discussed throughout this Report and Order.[445]

125. CTIA provides no explanation for its conclusory assertion that carriers' data privacy and security practices are not practices "in connection with" communications services.[446] Certainly any information collected from a customer or prospective customer related to establishing or maintaining the provision of a communications service would qualify. As discussed above, it is well established that carriers have come into possession of, and sometimes suffered breaches of, sensitive personal information that may not be CPNI.[447] Nor does the canon of statutory construction about specific provisions governing general ones apply here.[448] Section 222, adopted as part of the Telecommunications Act of 1996 (1996 Act), was not intended to narrow carriers' privacy duties or the Commission's authority to oversee carriers' privacy practices.[449] The Commission regulated carriers' privacy practices under its

[445] *1998 CPNI Order*, 13 FCC Rcd at 8066, para. 15 ("Based on the Act's grant of jurisdiction, the Commission has historically regulated the use and protection of CPNI by AT&T, the BOCs, and GTE, through the rules established in the *Computer III* proceedings. Sections 4(i), 201(b), and 303(r) of the Act authorize the Commission to adopt any rules it deems necessary or appropriate to carry out its responsibilities under the Act, so long as those rules are not otherwise inconsistent with the Act.").

[446] *See* CTIA Comments at 15. We are no more persuaded by arguments that take a different tack and contend that the carrier actions at issue in this proceeding are not "charges," "practices," "classifications," or "regulations" within the meaning of section 201(b). *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 6. This argument relies on the theory that the Supreme Court has held "that activity is not covered by Section 201(b) unless it '*resembles* activity that . . . transportation and communications agencies have long regulated.'" CTIA Dec. 6 *Ex Parte* at 6 (quoting *Global Crossing Telecomms., Inc. v. Metrophones Telecomms., Inc*., 550 U.S. 45, 55–58 (2007) (*Global Crossing*)). But in that decision, the Supreme Court did not so hold; it merely considered that factor in support of its threshold determination that the activity at issue there "easily fits within the language of the statutory phrase" as understood "in ordinary English." *Global Crossing*, 550 U.S. at 55. We see no reason why a carrier's privacy and data breach notification practices with respect to customer PII that it has by virtue of its service relationship with them would not easily fit within the ordinary understanding of that statutory phrase, as well. Independently, we also observe that the Commission has, in fact, historically regulated carriers' privacy practices under its section 201(b) authority. *See supra* note 442 and accompanying text.

[447] *See supra* para. 20.

[448] *See* CTIA Comments at 15.

[449] We reject contrary arguments premised on the fact that section 222 does not itself include a savings clause expressly preserving the Commission's authority under section 201, in contrast to section 251 of the Act. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 5. The 1996 Act made clear that "the amendments made by this Act shall not be construed to modify, impair, or supersede Federal, State, or local law unless expressly so provided in such Act or amendments." Telecommunications Act of 1996, Pub. L. 104-104, § 601(c)(1) (1996) (codified at 47 U.S.C. § 152 nt). Nothing in section 222 expressly modifies, impairs, or supersedes the Commission's authority under section 201(b) to act to ensure that carriers' practices are just and reasonable. While it is not entirely clear why Congress felt the need for an additional savings clause in section 251(i), it might simply have done so "to be doubly sure," *Barton v. Barr*, 140 S. Ct. 1442, 1453 (2020), particularly given the responsibilities assigned to the states in the implementation of sections 251 and 252 of the Act. *See generally* 47 U.S.C. §§ 251, 252. Nor are we persuaded by contrary claims based on high-level statements in legislative history about the balancing various interests underlying various legislative alternatives that eventually led to section 222 of the Act. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 5-6. Such high-level statements in legislative history do not persuade us to depart from what we see as the best interpretation of the statutory text. Nor is it even clear that the relevant balancing of interests in the cited legislative history necessarily is relevant to the particular exercise of section 201(b) authority at issue here. *See, e.g.*, H.R. Rep. No. 103-559, at 60 (June 24, 1994) (discussing the "careful balance of competing, often conflicting, considerations" of consumers' need "to be sure that information about them that carriers can collect is not misused" with consumers' expectation that "the carrier's employee will have available all relevant information about their service," which "argues for looser restrictions on internal use of customer information").

general Title II authority even before enactment of the 1996 Act,[450] and the 1996 Act codified the privacy duty and enacted specific restrictions for the new competitive environment that the Act was intended to promote.[451] As the Commission stated in 1998, "Congress … enacted section 222 to prevent consumer privacy protections from being inadvertently swept away along with the prior limits on competition."[452] For the reasons discussed throughout this Report and Order, notification to customers, law enforcement, and the Commission are essential to the Commission's oversight of carriers' privacy practices.

126. The structure of the Communications Act and its relationship with the Federal Trade Commission Act also demonstrate that this Commission has authority to make rules governing common carriers' protection of PII. The FTC has broad statutory authority to protect against "unfair or deceptive" acts or practices, but that authority is limited by carving out several exceptions for categories of entities subject to oversight by other regulatory agencies, one of which is common carriers subject to the Communications Act.[453] The clear intent is that the expert agencies in those areas will act based on the

[450] *See, e.g.*, *Application of Open Network Architecture and Nondiscrimination Safeguards to GTE Corp.*, Report and Order, 9 FCC Rcd 4922, para. 45 (1994) ("Our CPNI requirements reflect a careful balancing of customer privacy, efficiency, and competitive equity interests.").

[451] *See* H.R. Rep. No. 104-458, Joint Explanatory Statement of the Committee of Conference, 104th Cong., 2d Sess. 203-05. In the course of rejecting a request that carriers be compelled to share customer information with certain other carriers to protect against discrimination against competitors under sections 201(b) and 202(a) of the Act, the Commission stated that "the specific consumer privacy and consumer choice protections established in section 222 supersede the general protections identified in sections 201(b) and 202(a)." *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information et al.*, CC Docket No. 96-115 et al., Order on Reconsideration and Petitions for Forbearance, 14 FCC Rcd 14409, 14491, para. 153 (1999) (*1999 Order on Reconsideration*); *see also e.g.*, *Implementation of the Telecommunications Act of 1996, et al.*, CC Docket No. 96-115, *et al.*, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8073, para. 14 (1998) (*1998 Second Report and Order*) ("Congress established a comprehensive new framework in section 222, which balances principles of privacy and competition in connection with the use and disclosure of CPNI and other customer information."). Understood in context, that simply stands for the proposition that where consumer privacy issues addressed specifically in section 222 are implicated, the requirements of section 222 are controlling over more general protections in section 201(b) and 202(a) that are unrelated to privacy—such as advancing competitive neutrality. *See, e.g.*,*1999 Order on Reconsideration*, 14 FCC Rcd at 14491, para. 153 (explaining that "requiring the disclosure of CPNI to other companies to maintain competitive neutrality" under sections 201(b) and 202(a) "would defeat, rather than protect, customers' privacy expectations and control over their own CPNI" in contravention of "the specific consumer privacy and consumer choice protections established in section 222"). We similarly reject attempts to rely on statements about section 222 that the Commission made in analogous statutory contexts where it rejected pro-competition requirements under statutory provisions like sections 272 or 274 in light of the privacy requirements of section 222. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 6 (citing *1998 Second Report and Order*, 13 FCC Rcd at 8066-67, para. 4 (discussing the interplay of section 222 with sections 272 and 274) and *1999 Order on Reconsideration*, 14 FCC Rcd at 14485, para. 142 (discussing the interplay of sections 222 and 272)). More generally, to the extent that the Commission has made statements that its section 222 authority supersedes its authority under section 201(b), we disavow such an interpretation for the reasons stated in this section. Independently, with particular respect to data breach notification requirements, we do not find either section 201(b) or section 222 to be a more specific provision. And even assuming *arguendo* that section 222 were controlling within its self-described scope, our rules are fully consistent with that authority as well. *See supra* Section III.E.1.

[452] *1998 CPNI Order*, 13 FCC Rcd at 8061, para. 1.

[453] 15 U.S.C. § 44 (defining "Acts to regulate commerce" as including "the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto"); *id.* § 45(a)(2) (exempting from FTC authority "common carriers subject to the Acts to regulate commerce").

authorities provided by those agencies' statutes. It is implausible that Congress would have exempted common carriers from any obligation to protect their customers' private information that is not CPNI.[454]

3. Interconnected VoIP

127. We find that section 222 and our ancillary jurisdiction grant us authority to apply the rules we adopt today to interconnected VoIP providers. Interconnected VoIP providers have been explicitly subject to the Commission's data breach rules since 2007, when the Commission first adopted the data breach notification rule.[455] In the *2007 CPNI Order*, the Commission recognized that if interconnected VoIP services were telecommunications services, they self-evidently would be covered by section 222 and the Commission's implementing rules.[456] But because the Commission generally had not classified interconnected VoIP, the Commission also exercised its Title I ancillary jurisdiction to extend its CPNI rules to interconnected VoIP services, finding that "interconnected VoIP services fall within the subject matter jurisdiction granted to [the Commission] in the Act," and that "imposing CPNI obligations is reasonably ancillary to the effective performance of the Commission's various responsibilities."[457]

128. We proceed under the same alternative bases here, and conclude that legal and factual bases for the findings relied on in the *2007 CPNI Order* have only grown more persuasive since then. The Commission observed at the time that "interconnected VoIP service 'is increasingly used to replace analog voice service.'"[458] This trend has continued. Interconnected VoIP now accounts for a far larger share of the residential fixed voice services market than legacy switched access services, and "fixed switched access continues to decline while interconnected VoIP services continue to increase."[459] Therefore, as the Commission found in 2007, today's consumers should reasonably expect "that their telephone calls are private irrespective of whether the call is made using the services of a wireline carrier, a wireless carrier, or an interconnected VoIP provider, given that these services, from the perspective of a

[454] Insofar as some parties contend that section 222 establishes a comprehensive scheme of privacy regulation for carriers to the exclusion of section 201(b), yet also contest our interpretation of section 222(a), *see, e.g.*, NCTA Dec. 5, 2023 *Ex Parte* at 2-5; CTIA Dec. 6, 2023 *Ex Parte* at 2-6, they effectively ask us to accept that the supposedly comprehensive privacy scheme that Congress enacted intentionally left the non-CPNI PII of carriers' customers unprotected by federal law. As we discuss, we not only find that view contrary to the statutory text, but find it implausible more generally.

[455] *See 2007 CPNI Order*, 22 FCC Rcd at 6954-57, paras. 54-59; *see also* 47 CFR § 64.2003(o) (defining "telecommunications carrier or carrier" for purposes of the data breach rules to include interconnected VoIP providers).

[456] *2007 CPNI Order*, 22 FCC Rcd at 6954-55, para. 54. Although the Commission has not broadly addressed the statutory classification of interconnected VoIP as a general matter, it has consistently recognized that a provider may offer VoIP on a Title II basis if it voluntarily "holds itself out as a telecommunications carrier and complies with appropriate federal and state requirements." *IP-Enabled Services*; *E911 Requirements for IP-Enabled Service Providers*, WC Docket Nos. 04-36 and 05-196, First Report and Order and Notice of Proposed Rulemaking, 20 FCC Rcd 10245, 10268, para. 38 n.128 (2005), *aff'd sub nom. Nuvio Corp. v. FCC*, 473 F.3d 302 (D.C. Cir. 2006); *see also Connect America Fund et al.*, WC Docket No. 10-90 et al., Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 18143-44, para. 1389 ("[S]ome providers of facilities-based retail VoIP services state[d] that they are providing those services on a common carrier basis . . . .").

[457] *See 2007 CPNI Order*, 22 FCC Rcd at 6955, para. 55; *see also United States v. Southwestern Cable*, 392 U.S. 157, 177-78 (1968) (setting forth the two-part "ancillary jurisdiction" test); *Comcast Corp. v. FCC*, 600 F.3d 642, 654 (D.C. Cir. 2010) (holding that ancillary jurisdiction must be "necessary to further its regulation of activities over which [the Commission] does have express statutory authority").

[458] *See 2007 CPNI Order*, 22 FCC Rcd at 6956, para. 56.

[459] *Communications Marketplace Report*, GN Docket No. 22-203, FCC 22-103, at 120-21, para. 170 (2022) ("As of December 2021, residential fixed voice connections were about 28% switched access and 72% interconnected VoIP, with residential switched access connections comprising only 12.2% of all fixed retail voice connections.").

customer making an ordinary telephone call, are virtually indistinguishable."[460] We likewise think interconnected VoIP subscribers should reasonably expect their other information to also be protected and treated confidentially consistent with the other protections that apply under section 222. Furthermore, extending section 222's protections to interconnected VoIP service customers remains "necessary to protect the privacy of wireline or wireless customers that place calls to or receive calls from interconnected VoIP customers."[461] Indeed, following the *2007 CPNI Order*, Congress ratified the Commission's decision to apply section 222's requirements to interconnected VoIP services, adding language to section 222 that applied provisions of section 222 to users of "IP-enabled voice service."[462] These revisions to section 222 would not make sense if the privacy-related duties of subsections (a) and (c) did not apply to interconnected VoIP providers.[463]

129. In the case of interconnected VoIP providers that have obtained direct access to telephone numbers, we conclude that section 251(e) also gives us authority to condition that access on those providers' compliance with privacy requirements equivalent to those that apply to telecommunications carriers. The Commission previously exercised its authority under section 251(e) to ensure, for example, that an interconnected VoIP provider receiving direct access to numbers "possesses the financial, managerial, and technical expertise to provide reliable service."[464] Ensuring that interconnected VoIP providers remain on the same regulatory footing as telecommunications carriers with respect to customer privacy—as was the case when direct access to numbers for interconnected VoIP providers began—will ensure a level competitive playing field and ensure that consumers' expectations are met regarding the privacy of their information when using the telephone network.[465]

4. Legal Authority to Adopt Rules for TRS

130. We find that we have separate and independent authority under sections 225 and 222 to amend our data breach rule for TRS to ensure that TRS users receive privacy protections equivalent to those enjoyed by users of telecommunications and VoIP services. Section 225 of the Act directs the Commission to ensure that TRS are available to enable communication in a manner that is functionally equivalent to voice telephone services.[466] In the *2013 VRS Reform Order*, the Commission found that applying the privacy protections of the Commission's regulations to TRS users advances the functional equivalency of TRS.[467] The Commission concluded further that the specific mandate of section 225 to establish "functional requirements, guidelines, and operations procedures for TRS" authorizes the

[460] *2007 CPNI Order*, 22 FCC Rcd at 6956, para. 56.

[461] *Id.* at 6956, para. 57.

[462] *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283 (2008) (NET 911 Act); *see also* 47 U.S.C. § 222(d)(4), (f)(1), (g) (applying provisions of section 222 to "IP-enabled voice service" and defining "IP-enabled voice service" as having "the meaning given the term 'interconnected VoIP service' by section 9.3 of the Federal Communications Commission's regulations (47 CFR 9.3)"); *id.* § 615b(8).

[463] We note that no commenter chose to address this issue in the course of this proceeding.

[464] 47 CFR § 52.15(g)(3)(i)(F); *see also Numbering Policies for Modern Communications et al.*, WC Docket Nos. 13-97 et al., Report and Order, 30 FCC Rcd 6839, 6849-50, 6878-80, paras. 24, 78-82 (2015) (*2015 Direct Access to Numbering Order*).

[465] *See, e.g.*, *2015 Direct Access to Numbering Order*, 30 FCC Rcd at 6850-51, 6852-53, paras. 25, 28 (citing competitive neutrality as a benefit of the Commission's approach to providing interconnected VoIP providers direct access to numbers); *id*. at 6861, para. 47 (seeking to take account of customers' expectations).

[466] 47 U.S.C. § 225(a)(3), (b)(1).

[467] *2013 VRS Reform Order*, 28 FCC Rcd at 8685-86, para. 170.

Commission to make the privacy protections included in the Commission's data breach regulations applicable to TRS users.[468]

131. The Commission also found that extending its privacy—including data breach—regulations to TRS users was ancillary to its responsibilities under section 222 of the Act to telecommunications service subscribers that place calls to or receive calls from TRS users, because TRS call records include call detail information concerning all calling and called parties.[469] The Commission moreover determined that applying data breach requirements to point-to-point video services provided by VRS providers[470] is ancillary to its responsibilities under sections 222 and 225, including the need to protect information that VRS providers had by virtue of being a given customer's registered VRS provider—even in the context of point-to-point video service—and to guard against the risk to consumers who are likely to expect the same privacy protections when dealing with VRS providers, whether they are using VRS or point-to-point video services.[471]

132. We conclude that, for the same reasons cited in the *2013 VRS Reform Order*, these sources of authority for establishing the current data breach rule for TRS now authorize the Commission to amend this rule to ensure that TRS users continue to receive privacy protections equivalent to those enjoyed by users of telecommunications and VoIP services. The record in this proceeding supports this conclusion. As AARO states, the Commission has "ample legal authority" to amend its data breach rule for TRS under sections 222 and 225.[472]

5. Impact of the Congressional Disapproval of the *2016 Privacy Order*

133. In 2016, the Commission attempted to revise its breach notification rules as part of a larger proceeding addressing privacy requirements for broadband Internet service providers (ISPs).[473] The rules the Commission adopted in the *2016 Privacy Order* applied to telecommunications carriers and interconnected VoIP providers in addition to ISPs, which had been classified as providers of telecommunications services in 2015.[474] In 2017, however, Congress nullified those 2016 revisions to the Commission's privacy rules under the CRA.[475] Pursuant to the language of the Resolution of Disapproval, the *2016 Privacy Order* was rendered "of no force or effect."[476] That resolution conformed

[468] *Id.* at 8685-86, para. 170 & n.430 (citing 47 U.S.C. § 225(d)(1)(A)).

[469] *2013 VRS Reform Order*, 28 FCC Rcd at 8685-86, para. 170.

[470] Such point-to-point services, while provided in association with VRS, are not themselves a form of TRS.

[471] *2013 VRS Reform Order*, 28 FCC Rcd at 8686-87, para. 171.

[472] AARO Comments at 4; *see also* Hamilton Relay Comments at 9 (stating that section 225 "provides sufficient authority to impose CPNI data breach notification obligations on TRS providers"); EPIC et al. Reply at 17.

[473] *2016 Privacy Order*, 31 FCC Rcd at 14019-33, paras. 261-291. In 2015, the Commission classified broadband Internet access service as a telecommunications service subject to Title II of the Act, a decision that the D.C. Circuit upheld in *U.S. Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016). *See Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5733-34, paras. 306-308 (2015), *aff'd*, *U.S. Telecom Ass'n v. FCC*, 825 F.3d 674 (D.C. Cir. 2016). As a result of classifying broadband Internet access service as a telecommunications service, such services were subject to sections 201 and 222 of the Act.

[474] *See 2016 Privacy Order*, 31 FCC Rcd at 13925, para. 39, 14033-34, para. 293. In 2017, the Commission reversed the 2015 classification decision so that Title II obligations, including section 222, no longer apply to ISPs. *Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report and Order, and Order, 33 FCC Rcd 311 (2017), *aff'd in part and remanded in part*, *Mozilla Corp. v. FCC*, 940 F.3d 1 (D.C. Cir. 2019), *on remand*, Order on Remand, 35 FCC Rcd 12328 (2020), *ptns. for recon. pending*.

[475] *See* Resolution of Disapproval; 5 U.S.C. § 801(b)(1), (f); *see also 2017 CRA Disapproval Implementation Order*.

[476] Resolution of Disapproval.

to the procedure set out in the CRA, which requires agencies to submit most rules to Congress before they can take effect and provides a mechanism for Congress to disapprove of such rules. Pursuant to the operation of the CRA, the *2016 Privacy Order* "may not be reissued in substantially the same form, and a new rule that is substantially the same as such a rule may not be issued, unless the reissued or new rule is specifically authorized by a law enacted after the date of the joint resolution disapproving the original rule."[477]

134. In analyzing the impact of the Resolution of Disapproval of the *2016 Privacy Order*, we first explain our understanding of the CRA's prohibition on reissuance. We also show that, in any event, the revisions that we make here to the breach notification rule are different in substantial ways from those that were included in the *2016 Privacy Order*.

135. First, we conclude that the CRA is best interpreted as prohibiting the Commission from reissuing the *2016 Privacy Order* in whole, or in substantially the same form, or from adopting another item that is substantially the same as the *2016 Privacy Order*. It does not prohibit the Commission from revising its breach notification rules in ways that are similar to, or even the same as,[478] some of the revisions that were adopted in the *2016 Privacy Order*, unless the revisions adopted are the same, in substance, as the *2016 Privacy Order* as a whole.[479]

136. Congress's Resolution of Disapproval, by its terms, disapproved "the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services' (81 Fed. Reg. 87274 (December 2, 2016))."[480] This referred to the *2016 Privacy Order* in its entirety, which was summarized in the cited *Federal Register* document. The statutory term "rule," as used in the CRA, refers to "the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency."[481] Thus, "rule" can and does refer to an entire decision that adopts rules.[482] The term "rule" can also refer to parts of such

[477] 5 U.S.C. § 801(b)(2).

[478] To be clear, although the CRA would permit the Commission to adopt a breach notification rule that is the same as the breach notification rule that was adopted by the *2016 Privacy Order*, the rule that we adopt here today has substantial differences.

[479] We reject arguments that there was insufficient notice for the Commission to adopt this interpretation of the effect of the CRA resolution of disapproval. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 8. In pertinent part, notice under the APA requires "reference to the legal authority under which the rule is proposed" and "either the terms or substance of the proposed rule or a description of the subjects and issues involved." 5 U.S.C. § 553(b)(2), (3). The *Data Breach Notice* described the proposal to adopt expanded data breach notification requirements pursuant to its statutory authority under sections 222, 225, and other possible sources of authority. *See generally Data Breach Notice* at 1-26, paras. 1-61. In the course of this request for comment, the Commission sought specific comment regarding "the effect and scope of the Congressional disapproval of the *2016 Privacy Order*." *Id.* at 24, para. 52. This satisfies the requirements of the APA. Even beyond that, however, our interpretation flows from ordinary tools of statutory interpretation, first and foremost by focusing on the relevant statutory text and context. Contrary to the suggestion of some, *see* CTIA Dec. 6, 2023 *Ex Parte* at 8, we find nothing "novel" about this interpretive approach, providing additional grounds to conclude that the notice and comment requirements of the APA were satisfied here.

[480] Resolution of Disapproval.

[481] 5 U.S.C. § 804(3) (incorporating the definition of "rule" in 5 U.S.C. § 551, with exclusions); *id.* § 551(4) (defining "rule").

[482] In implementing Congress's resolution of disapproval, the Commission treated the *2016 Privacy Order* as a single rule. In a ministerial order, the Commission "simply recogniz[ed] the effect of the resolution of disapproval" should be that "the *2016 Privacy Order* 'shall be treated as though [it] had never taken effect.'" As a result, all of the changes that the *2016 Privacy Order* made to the Commission rules codified in the Code of Federal Regulations were reversed, with the result that all of the Commission rules in part 64, subpart U, were restored to how they read (continued….)

a decision, or to various requirements as adopted or amended by such a decision. In the context of the CRA's bar on reissuance, we must consider which rule is specified by that bar. The reissuance bar, 5 U.S.C. § 801(b)(2), provides that "a new rule that is substantially the same as such a rule may not be issued"—where "such a rule" refers to the rule specified in the joint resolution of disapproval as described in section 802.[483] As shown above, the joint resolution referred to the entirety of the *2016 Privacy Order*. Therefore, we conclude that the "rule" to which the reissuance bar applies is the entire *2016 Privacy Order* with all of the rule revisions adopted therein.[484]

137. We conclude that it would be erroneous to construe the resolution of disapproval as applying to anything other than all of the rule revisions, as a whole, adopted as part of the *2016 Privacy Order*. That resolution had the effect of nullifying each and every provision of the *2016 Privacy Order*—each of those parts being rules under the APA—but not "the rule" specified in the resolution of disapproval. By its terms, the CRA does not prohibit the adoption of a rule that is merely substantially similar to a limited portion of the disapproved rule or one that is the same as individual pieces of the disapproved rule.[485]

138. To prohibit an agency from making any of the individual decisions made in an entire disapproved rulemaking action would not only be contrary to the text of the resolution of disapproval, interpreted consistently with the CRA, but also would be contrary to the apparent intent of the CRA. When Congress adopted the CRA, it recognized that it would be necessary for agencies to interpret the scope of the bar on reissuance in the future. According to a floor statement that its authors intended to be authoritative,

(Continued from previous page)
prior to their amendment by the *2016 Privacy Order*. *2017 CRA Disapproval Implementation Order*, 32 FCC Rcd at 5442-43 paras. 2, 3 (quoting 5 U.S.C. § 801(f)) (second alteration in original).

[483] 5 U.S.C. § 801(b)(2); *see also id.* § 802.

[484] Because it is contrary to our understanding of the appropriate focus under the CRA, we reject arguments that we must conduct the 5 U.S.C. § 801(b)(2) evaluation by reference specifically to the breach notification rule from the *2016 Privacy Order*. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 7.

[485] *See generally* Michael J. Cole, *Interpreting the Congressional Review Act: Why the Courts Should Assert Judicial Review, Narrowly Construe "Substantially the Same," and Decline to Defer to Agencies Under* Chevron, 70 Admin. L. Rev. 53, 83-94 (2018) (arguing for a narrow interpretation of "substantially the same"). We reject arguments that because the CRA borrows from the APA's definition of "rule" as referring to the whole or a part of certain agency statements of general applicability and future effect, an agency cannot adopt a rule substantially similar to any part of an agency rulemaking decision that does not take effect due to a resolution of disapproval under the CRA. *See, e.g.*, CTIA Dec. 6 *Ex Parte* at 8. The key issue is not the definition of "rule" in the abstract, but the wording of 5 U.S.C. § 801(b)(2) (along with the wording of the resolution of disapproval itself). And 5 U.S.C. § 801(b)(2) is worded in singular terms—referring to "*A rule* that does not take effect (or does not continue) under paragraph (1) . . . " as opposed to saying "*Any rule* that does not take effect (or does not continue) under paragraph (1) . . . " or "*Rules* that do not take effect (or do not continue) under paragraph (1) . . . ." So even if there might be multiple APA rules that do not take effect as a result of a resolution of disapproval, the CRA's focus is on a singular "rule" that does not take effect. Since the whole *2016 Privacy Order* was the subject of the resolution of disapproval, and the whole *2016 Privacy Order* did not take effect as a result, we conclude that the whole *2016 Privacy Order* is the relevant "rule" for purposes of 5 U.S.C. § 801(b)(2). And although some commenters claim that our approach to interpreting the CRA could lead to uncertainty about what is subject to 5 U.S.C. § 801(b)(2), they do not identify any actual ambiguity as our approach is applied here—instead, they seemingly just dislike the outcome. *See, e.g.*, CTIA Dec. 6, 2024 *Ex Parte* at 8-9. Nor are we persuaded that Congress lacks the tools to address any concerns about the scope of a resolution of disapproval if any were to arise. *See* Dissenting Statement of Commissioner Carr at 1. For example, the record does not reveal why Congress could not specify the "relating to" criterion in the resolution of disapproval language required by 5 U.S.C. § 802(a) in more granular or detailed ways. Independently, Congress also always remains free to enact laws outside the CRA process that reject agency rules with as much detail and precision as they wish should ambiguity concerns become a practical problem.

> [t]he authors [of the CRA] intend the debate on any resolution of disapproval to focus on the law that authorized the rule and make the congressional intent clear regarding the agency's options or lack thereof after enactment of a joint resolution of disapproval. It will be the agency's responsibility in the first instance when promulgating the rule to determine the range of discretion afforded under the original law and whether the law authorizes the agency to issue a substantially different rule. Then, the agency must give effect to the resolution of disapproval.[486]

139. Accordingly, we observe that, in the floor debate on the resolution of disapproval in 2017, supporters of the resolution did not mention the breach notification provision apart from a brief reference.[487] Senators who spoke in favor of the resolution cited the *2016 Privacy Order*'s treatment of broadband providers and the information they hold as different from providers of other services on the internet.[488] The debate gives no reason to believe that the breach notification rule motivated those members of Congress who supported the resolution.[489]

140. As EPIC notes in its comments, Congressional disapproval of the *2016 Privacy Order* under the CRA was largely predicated on claims that the Order would create duplicative privacy authority with the Federal Trade Commission as relates to broadband Internet service providers.[490] A review of the Congressional record from 2017 reveals that this indeed appears to have been the animating justification

---

[486] Statement for the Record by Senators Nickles, Reid, and Stevens, 142 Cong. Rec. S3686 (Apr. 18, 1996) (post-enactment).

[487] *See Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission*, 163 Cong. Rec. S1925-55 (daily ed. Mar. 22, 2017), https://www.congress.gov/congressional-record/2017/3/22/senate-section/article/S1925-2; *Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission*, 163 Cong. Rec. H2478-86 (daily ed. Mar. 28, 2017), https://www.congress.gov/congressional-record/volume-163/issue-54/house-section/article/H2478-1. *But see* 163 Cong. Rec. H2479 (daily ed. Mar. 28, 2017) (statement of Rep. Burgess) (referencing the 2016 data breach consumer notice requirements among many other aspects of the *2016 Privacy Order*),

[488] *Id.*

[489] *See* Adam M. Finkel & Jason W. Sullivan, *A Cost-Benefit Interpretation of the "Substantially Similar" Hurdle in the Congressional Review Act: Can OSHA Ever Utter the E-Word (Ergonomics) Again?*, 63 Admin. L. Rev. 707, 740-41 (2011) (arguing that, because a resolution of disapproval must be all-or-nothing, a "far-reaching interpretation of 'substantially the same' would limit an agency's authority in ways Congress did not intend in exercising the veto"), *cited in* Cole, *supra* note 485, at 89. Although our conclusion that the whole *2016 Privacy Order* is the relevant "rule" for purposes of 5 U.S.C. § 801(b)(2) is fully justified even without considering the legislative history of the resolution of disapproval, we reject arguments that it is inappropriate to also look at that history and contentions that we are misinterpreting that history. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 9; AT&T Dec. 6, 2023 *Ex Parte* at 2. In addition to legislative history of the CRA that indicates that the legislative history of each resolution of disapproval should be relevant, out of an abundance of caution given the lack of an authoritative determination specifying the details of how to evaluate whether a rule is substantially the same under 5 U.S.C. § 801(b)(2), we consider whether there are indicia from the legislative history of the resolution of disapproval here to inform that analysis. For instance, if the legislative history indicated that the resolution of disapproval of the *2016 Privacy Order* somehow hinged entirely or significantly on concern about some or all of the 2016 data breach reporting requirements, we then could consider whether and how to account for that in the 5 U.S.C. § 801(b)(2) analysis notwithstanding the fact that there is little practical overlap between this order and the entirety of the *2016 Privacy Order*. Although data breach notification issues occasionally appear to have been raised by of opponents of the resolution of disapproval, high-level statements by supporters of the resolution about "FCC overreach" or the like do not, without more, persuade us that the 2016 data breach notification requirements played a significant role in motivating the resolution of disapproval. Thus, we see nothing in the legislative history of the resolution of disapproval that would cause us to question our conclusion that our action here does not adopt substantially the same rule for CRA purposes.

[490] *See* EPIC Comments at 12; *Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission*, 163 Cong. Rec. H2489, H2489 (2017) (statement of Rep. Blackburn).

for Congressional disapproval of the *2016 Privacy Order*.[491] Whatever the merits of such an argument, we find that it does not now preclude us from adopting the rules set forth in this Order. As EPIC notes, the rules we adopt today are not privacy measures directed at broadband Internet service providers, but rather, data security measures directed at providers of telecommunications, interconnected VoIP services, and TRS, and which build upon rules that have existed since 2007.[492] Thus, the primary animating justification behind Congressional disapproval of the *2016 Privacy Order* is irrelevant to the present case.

141. In addition, the revisions that we make here to the breach notification rule are different in substantial ways from those that Congress disapproved in 2017. The *2016 Privacy Order* was focused in large part on adopting privacy rules for broadband Internet access service, and also made a number of changes to the Commission's privacy rules more generally that, among other things, required carriers to disclose their privacy practices, revised the framework for customer choice regarding carriers' access, use, and disclosure of the customers' information, and imposed data security requirements in addition to data breach notification requirements.[493] When the *2016 Privacy Order* is viewed as a whole, it is clear that there is at most a small conceptual overlap between the adoption of data breach notification requirements at issue here and the many actions taken in that *Order* of which data breach notification requirements represented only a small fraction.

142. Independently, even assuming *arguendo* that the CRA were interpreted to require an evaluation on a more granular basis here, we are not persuaded that the requirements we adopt here are substantially the same as analogous requirements in the *2016 Privacy Order*.[494] For example, the customer notification requirement we adopt here is materially less prescriptive regarding the content and manner of customer notice than what the Commission adopted in 2016.[495] Further, the 2016 data breach notification rules for customer notifications and government agency notifications did not incorporate the good-faith exception from the definition of covered breaches that we adopt here.[496] With respect to the federal agency notification requirements, as compared to the 2016 rules, the rules we adopt here in that regard provide for the Commission and other law enforcement agencies to gain a much more complete picture of data breaches, including trends and emerging activities, consistent with the demonstrated need for such oversight.[497] Consequently, even assuming *arguendo* that one were to conduct the 5 U.S.C. § 801(b)(2) evaluation on a more granular basis, we are not persuaded that the data breach notification requirements we adopt here would be substantially the same as breach notification requirements adopted in the *2016 Privacy Order*.[498]

---

[491] *See, e.g.*, *Providing for Congressional Disapproval of a Rule Submitted by the Federal Communications Commission*, 163 Cong. Rec. H2489, H2489 (2017) (statement of Rep. Blackburn) (arguing that the Commission had "unilaterally swiped jurisdiction from the Federal Trade Commission [(FTC)]," that the "FTC has served as our Nation's sole online privacy regulator for over 20 years," and that "having two privacy cops on the beat will create confusion within the internet ecosystem and will end up harming consumers").

[492] EPIC Comments at 12.

[493] *See, e.g.*, *2016 Privacy Order*, 31 FCC Rcd at 13913-16, paras. 6-18 (summarizing the actions and decisions in the *2016 Privacy Order*).

[494] *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* Letter at 7.

[495] *See, e.g.*, *2016 Privacy Order*, 31 FCC Rcd at 14085, Appx. A (section 64.2006(a) specifying customer notification requirements).

[496] *See, e.g.*, *id*. at 14080, Appx. A (section 64.2002(c) defining "breach of security," "breach," or "data breach").

[497] *See, e.g.*, *id*. at 14085, Appx. A (section 64.2006(b), (c) providing for the Commission, FBI, and Secret Service to receive breach notifications, but only for breaches affecting 5,000 or more customers and only if the carrier does not reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach).

[498] Even assuming one were to conduct the 5 U.S.C. § 801(b)(2) evaluation at a more granular basis, we are not persuaded that the breach notification rule from the *2016 Privacy Order* is the right level of granularity, nor that the evaluation of whether rules are substantially the same should be conducted based on high-level policy similarities, as (continued….)

143. Nor are we adopting something substantially the same as the *2016 Privacy Order* as a whole through the aggregate effect of individual Commission actions.[499] For one, the theory that classification of broadband Internet access service as a telecommunications service will automatically subject those services to our privacy rules, including the data breach notification requirements adopted here, is belied by multiple considerations: (1) the Commission has simply sought comment on those classification issues in its *Open Internet Notice* and has not yet acted in that regard;[500] (2) the *2015 Open Internet Order* shows that the Commission is willing and able to decline to apply rules that might be triggered by a classification decision, having done so there, for example, by forbearing from all rules implementing section 222 pending consideration in a subsequent proceeding;[501] and (3) the *Open Internet Notice* sought comment on following the same approach to privacy that the Commission took in the *2015 Open Internet Order* and specifically noted the resolution of disapproval of the *2016 Privacy Order* as a relevant consideration bearing on how it proceeds there.[502] Our analysis also is not materially altered by arguments that the Commission otherwise has adopted "data security, customer authentication, employee training, and other requirements."[503] In addition to being unpersuaded that such requirements substantially "mirror provisions of the 2016 order,"[504] we independently are not persuaded that the aggregation of such requirements and the data breach notification requirements adopted here lead to such a significant overlap with the *2016 Privacy Order* as to render our collective actions substantially the same as the *2016 Privacy Order* as a whole.[505]

(Continued from previous page)
some commenters contend. *See, e.g.*, CTIA Dec. 6, 2023 *Ex Parte* at 7. For example, the customer notification requirement is itself a "rule" within the meaning of the APA, as is the federal agency notification requirement. Ultimately, however viewed, we are persuaded that the rules we adopt here are not substantially the same as a disapproved rule for purposes of the CRA.

[499] *See* Dissenting Statement of Commissioner Simington at 1.

[500] *See generally Safeguarding and Securing the Open Internet*, WC Docket No. 23-320, Notice of Proposed Rulemaking, FCC 23-83 (Oct. 20, 2023) (*Open Internet Notice*).

[501] *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order, Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5823-24, para. 467 (2015) (*2015 Open Internet Order*).

[502] *Open Internet Notice*, FCC 23-83, para. 104 & n.352.

[503] Dissenting Statement of Commissioner Simington at 1.

[504] Dissenting Statement of Commissioner Simington at 1. For example, in the recent *SIM Swap Order*, the Commission adopted certain privacy requirements focused on wireless carriers' practices in the specific context of account transfers (or "swaps") from a device associated with one subscriber identity module (SIM) to a device associated with a different SIM on in connection with a wireless number being ported out. *Protecting Consumers from SIM Swap and Port-Out Fraud*, WC Docket No. 21-341, Report and Order and Further Notice of Proposed Rulemaking, FCC 23-95 (Nov. 16, 2023). That is a vastly different focus than the *2016 Privacy Order*, which focused on the general privacy practices of all carriers. *See generally 2016 Privacy Order*. Thus, even assuming *arguendo* some high-level conceptual similarities, the operation and practical effect is significantly different than even arguably analogous requirements that were part of the *2016 Privacy Order*.

[505] As discussed above, the primary focus of the *2016 Privacy Order* was privacy rules for broadband Internet access service, along with a number of changes to the Commission's privacy rules more generally that, among other things, required carriers to disclose their privacy practices, and revised the framework for customer choice regarding carriers' access, use, and disclosure of the customers' information. *See supra* note 493 and accompanying text. Given the other significant issues central to that decision, even assuming *arguendo* that there were some conceptual overlap between the issues addressed in the *2016 Privacy Order* and data security, customer authentication, and employee training requirements recently adopted by the Commission—and even considered in conjunction with the data breach notification rules we adopt here—we are not persuaded that the Commission has adopted substantially the same rule as the *2016 Privacy Order*. Separately, insofar as we consider the legislative history of the 2017 resolution of disapproval, data security, customer authentication, and employee training requirements likewise received only isolated mention, and then primarily with respect to broadband Internet access service. *See* 163 Cong.
(continued….)

IV. EFFECTIVE DATES

144. The revised recordkeeping and reporting requirements adopted in this Report and Order, including the revisions to 47 CFR §§ 64.2011 and 64.5111 set forth in Appendix A, are subject to approval by the Office of Management and Budget (OMB). Unless and until such time as OMB approves these new or modified requirements, the current, unmodified versions of 47 CFR §§ 64.2011 and 64.5111 shall continue to apply.

145. We direct the Wireline Competition Bureau to announce OMB approval and effective dates for the modified rules contained within this Order by subsequent public notice. Pursuant to this process, we anticipate that carriers of all sizes will have ample time to come into compliance with these requirements, and therefore reject CCA's request for a 12-month implementation timeline.[506]

V. PROCEDURAL MATTERS

146. *Final Regulatory Flexibility Analysis*. Pursuant to the Regulatory Flexibility Act of 1980 (RFA), as amended,[507] the Commission's Final Regulatory Flexibility Analysis is set forth in Appendix B. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this Report and Order, including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[508]

147. *Paperwork Reduction Act.* This document contains new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. All such new or modified requirements will be submitted to OMB for review under section 3507(d) of the PRA.[509] OMB, the general public, and other federal agencies will be invited to comment on any new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 47 U.S.C.

(Continued from previous page)
Rec. S1928 (daily ed. Mar. 22, 2017) (statement of Sen. Thune) (noting calls "for returning jurisdiction over broadband providers' privacy and data security practices to the FTC"); 163 Cong. Rec. H2485 (Mar. 28, 2017) (statement of Rep. Burgess) (including an op-ed in the record expressing concern about the loss of the FTC as "America's sole online privacy regulator" that enforced "privacy and data-security requirements"). Consequently, that legislative history does not reveal that the resolution of disapproval hinged entirely or significantly on concerns about such issues, even considered collectively. Thus, whether viewed alone or in the aggregate, we are not persuaded that we have adopted substantially the same rule as the *2016 Privacy Order* as a whole. *Cf.* Securities and Exchange Commission, *Disclosure of Payments by Resource Extraction Issuers*, 86 Fed. Reg. 4662, 4665 (Jan. 15, 2021) (ensuring that the new rule adopted there was not substantially the same as the rule previously subject to a resolution of disapproval under the CRA "is reasonably achieved by changing at least one of the two central discretionary determinations at the heart of the" previously disapproved rule and effectuating that by "requir[ing] less granularity in the payment disclosures than in the disapproved rule," which was itself "sufficient to comply with the CRA's requirements that the disapproved rule not be reissued in 'substantially the same form' and a new rule may not be 'substantially the same' as the disapproved rule."). And we note, of course, that Congressional disapproval of a particular rule implementing a statute does not nullify an agency's general authority under that statute. *Id.*; 142 Cong. Rec. S3686 (daily ed. Apr. 18, 1996) ("If the law that authorized the disapproved rule provides broad discretion to the issuing agency regarding the substance of such rule, the agency may exercise its broad discretion to issue a substantially different rule. If the law that authorized the disapproved rule did not mandate the promulgation of any rule, the issuing agency may exercise its discretion not to issue any new rule. Depending on the law that authorized the rule, an issuing agency may have both options.").

[506] *See* CCA Dec. 8, 2023 *Ex Parte* at 3.

[507] *See* 5 U.S.C. § 603.

[508] *See id.* § 603(a).

[509] *See* NCTA Dec. 5, 2023 *Ex Parte* at 7 (requesting clarification as to which of the rules in the Order will be submitted to OMB for approval); CCA Dec. 8, 2023 *Ex Parte* at 2-3; *see also* CTIA Dec. 6, 2023 *Ex Parte* at 16 n.107.

3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.[510]

148. In this Report and Order, we have assessed the effects of (1) expanding the scope of the data breach notification rules to cover specific categories of PII that carriers hold with respect to their customers; (2) expanding the definition of "breach" to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier, and such information is not used improperly or further disclosed; (3) requiring carriers to notify the Commission, in addition to Secret Service and FBI, as soon as practicable, and in no event later than seven business days after reasonable determination of a breach; (4) eliminating the requirement that carriers notify customers of a breach in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involved encrypted data and the carrier had definitive evidence that the encryption key was not also accessed, used, or disclosed; and (5) applying similar rules to TRS providers, and we find that the impact on small businesses with fewer than 25 employees will be minimal. While the Commission expanded the scope of the data breach notification rules, we also adopted a good-faith exception from the definition of breach which limits the reportable instances. Additionally, the Commission decided to utilize the existing reporting portal, which small carriers and TRS providers are already accustomed to using, for federal agency breach notifications rather than creating a new centralized portal. The Commission delegated authority to the Wireline Competition Bureau to coordinate with the Secret Service, the current administrator of the reporting facility, and the FBI, to the extent necessary, to ensure that the Commission will be notified when data breaches are reported, thereby ensuring that no additional burden would be imposed on small and other carriers and TRS providers from separate reporting requirements. We also exempted from the federal agency reporting requirement breaches that affect fewer than 500 customers and for which the carrier reasonably determines that no harm to customers is reasonably likely to occur, and instead require carriers to file with federal agencies an annual summary regarding all such breaches occurring in the previous calendar year. This annual reporting requirement is intended to minimize the burden of reporting such breaches to federal law enforcement and the Commission. In determining the content and format requirements of the annual report, the Commission instructed the Bureau to minimize the burdens on carriers and TRS providers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. Additionally, with the support of several small carriers, the Commission adopted a harm-based notification trigger for reporting breaches to customers, which allows small providers to focus their resources on data security and mitigation measures rather than generating notifications where harm to the consumer is unlikely.

149. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, concurs, that this rule is non-major under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a copy of this Report and Order to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

150. *OPEN Government Data Act*. The OPEN Government Data Act,[511] requires agencies to make "public data assets" available under an open license and as "open Government data assets," *i.e.*, in machine-readable, open format, unencumbered by use restrictions other than intellectual property rights, and based on an open standard that is maintained by a standards organization.[512] This requirement is to be

[510] *See* 44 U.S.C. § 3506(c)(4).

[511] Congress enacted the OPEN Government Data Act as Title II of the Foundations for Evidence-Based Policymaking Act of 2018, Pub. L. No. 115-435 (2019), §§ 201-202.

[512] 44 U.S.C. § 3502(20), (22) (definitions of "open Government data asset" and "public data asset"); *id.* § 3506(b)(6)(B) (public availability).

implemented "in accordance with guidance by the Director" of the OMB.[513] The term "public data asset" means "a data asset, or part thereof, maintained by the Federal Government that has been, or may be, released to the public, including any data asset, or part thereof, subject to disclosure under [the Freedom of Information Act (FOIA)]."[514] A "data asset" is "a collection of data elements or data sets that may be grouped together,"[515] and "data" is "recorded information, regardless of form or the media on which the data is recorded."[516] We delegate authority, including the authority to adopt rules, to the Wireline Competition Bureau, in consultation with the agency's Chief Data Officer and after seeking public comment to the extent it deems appropriate, to determine whether to make publicly available any data assets maintained or created by the Commission pursuant to the rules adopted herein, and if so, to determine when and to what extent such information should be made publicly available. In doing so, the Bureau shall take into account the extent to which such data assets should not be made publicly available because they are not subject to disclosure under the FOIA.[517]

151. *People with Disabilities.* To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice).

152. *Contact Person.* For further information, please contact Mason Shefa, Competition Policy Division, Wireline Competition Bureau, at (202) 418-2494 or mason.shefa@fcc.gov.

VI. ORDERING CLAUSES

153. Accordingly, IT IS ORDERED that, pursuant to sections 1, 2, 4(i), 4(j), 201, 202, 222, 225, 251, 303(b), 303(r), 332, and 705 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152, 154(i), 154(j), 201, 202, 222, 225, 251, 303(b), 303(r), 332, 605, this Report and Order IS ADOPTED.

154. IT IS FURTHER ORDERED that part 64 of the Commission's rules IS AMENDED as set forth in Appendix A.

155. IT IS FURTHER ORDERED that this Report and Order SHALL BE effective thirty (30) days after publication of the text or a summary thereof in the Federal Register, except that the amendments to 47 CFR §§ 64.2011 and 64.5111, which contain new or modified information collection requirements that require approval by the Office of Management and Budget under the Paperwork Reduction Act, will not be effective until the Office of Management and Budget completes any required review under the Paperwork Reduction Act. The Commission directs the Wireline Competition Bureau to publish a notice in the Federal Register announcing completion of such review and the relevant effective date. It is our intention in adopting the foregoing Report and Order that, if any provision of the Report and Order or the rules, or the application thereof to any person or circumstance, is held to be unlawful, the remaining portions of such Report and Order and the rules not deemed unlawful, and the application of such Report and Order and the rules to other person or circumstances, shall remain in effect to the fullest extent permitted by law.

156. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, Reference Information Center, SHALL SEND a copy of this Report and Order to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

[513] OMB has not yet issued final guidance.

[514] 44 U.S.C. § 3502(22).

[515] *Id.* § 3502(17).

[516] *Id.* § 3502(16).

[517] *See, e.g.*, 5 U.S.C. § 552(b)(4), (6)-(7) (exemptions concerning confidential commercial information, personal privacy, and information compiled for law enforcement purposes, respectively).

157. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, Reference Information Center, SHALL SEND a copy of this Report and Order, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

For the reasons discussed above, the Federal Communications Commission part 64 of Title 47 of the Code of Federal Regulations as follows:

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

1. The authority citation for part 64 continues to read as follows:

Authority: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 620, 716, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091.

2. Amend Subpart U by revising the Subpart heading to read as follows:

Subpart U – Privacy of Customer Information

3. Amend § 64.2011 by revising paragraphs (a) through (e) to read as follows:

§ 64.2011 Notification of security breaches.

(a) *Commission and Federal Law Enforcement Notification.* Except as provided in paragraph (a)(3) of this section, as soon as practicable, but no later than seven business days, after reasonable determination of a breach, a telecommunications carrier shall electronically notify the Commission, the United States Secret Service (Secret Service), and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility on its website.

(1) A telecommunications carrier shall, at a minimum, include in its notification to the Commission, Secret Service, and FBI:

(i) the carrier's address and contact information;

(ii) a description of the breach incident;

(iii) the method of compromise;

(iv) the date range of the incident;

(v) the approximate number of customers affected;

(vi) an estimate of financial loss to the carrier and customers, if any; and

(vii) the types of data breached.

(2) If the Commission, or a law enforcement or national security agency, notifies the carrier that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security.

(3) A telecommunications carrier is exempt from the requirement to provide notification to the Commission and law enforcement pursuant to paragraph (a) of this section of a breach that affects fewer than 500 customers and the carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. In circumstances where a carrier initially determined that it qualified for an exemption under this subsection, but later discovers information such that this exemption no longer applies, the carrier must report the breach to federal agencies as soon as practicable, but no later than within seven business days of this discovery, as required in

paragraph (a).

(b) *Customer Notification.* Except as provided in paragraph (a)(2) of this section, a telecommunications carrier shall notify affected customers of a breach of covered data without unreasonable delay after notification to the Commission and law enforcement pursuant to paragraph (a) of this section, and no later than 30 days after reasonable determination of a breach. This notification shall include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. Notwithstanding the foregoing, customer notification shall not be required where a carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed.

(c) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Commission, Secret Service, and the FBI pursuant to paragraph (a) of this section, and notifications made to customers pursuant to paragraph (b) of this section. The record shall include, if available, dates of discovery and notification, a detailed description of the covered data that was the subject of the breach, the circumstances of the breach, and the bases of any determinations regarding the number of affected customers or likelihood of harm as a result of the breach. Carriers shall retain the record for a minimum of 2 years.

(d) *Annual Reporting of Certain Small Breaches.* A telecommunications carrier shall have an officer, as an agent of the carrier, sign and file with the Commission, Secret Service, and FBI, a summary of all breaches occurring in the previous calendar year affecting fewer than 500 individuals and where the carrier could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. This filing shall be made annually, on or before February 1 of each year, through the central reporting facility, for data pertaining to the previous calendar year.

(e) *Definitions.*

(1) As used in this section, a "breach" occurs when a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data. A "breach" shall not include a good-faith acquisition of covered data by an employee or agent of a telecommunications carrier where such information is not used improperly or further disclosed.

(2) As used in this section, "covered data" includes both a customer's CPNI, as defined by § 64.2003, and personally identifiable information.

(3) As used in this section, "encrypted data" means covered data that has been transformed through the use of an algorithmic process into a form that is unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.

(4) As used in this section, "encryption key" means the confidential key or process designed to render encrypted data useable, readable, or decipherable.

(5) Except as provided in paragraph (e)(6) of this section, as used in this section, "personally identifiable information" means:

(i) An individual's first name or first initial, and last name, in combination with any government-issued identification numbers or information issued on a government document used to verify the identity of a specific individual, or other unique identification number used for authentication purposes;

(ii) An individual's user name or e-mail address, in combination with a password or security question and answer, or any other authentication method or information necessary to permit access to an account; or

(iii) Unique biometric, genetic, or medical data.

(iv) Notwithstanding the above:

(A) Dissociated data that, if linked, would constitute personally identifiable information is to be considered personally identifiable if the means to link the dissociated data were accessed in connection with access to the dissociated data; and

(B) Any one of the discrete data elements listed in paragraphs (e)(5)(i) to (iii) of this section, or any combination of the discrete data elements listed above is personally identifiable information if the data element or combination of data elements would enable a person to commit identity theft or fraud against the individual to whom the data element or elements pertain.

(6) As used in this section, "personally identifiable information" does not include information about an individual that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

* * * * *

4. Amend § 64.5111 by revising paragraphs (a) through (e) to read as follows:

§ 64.5111 Notification of security breaches.

(a) *Commission and Federal Law Enforcement Notification.* Except as provided in paragraph (a)(3) of this section, as soon as practicable, but not later than seven business days, after reasonable determination of a breach, a TRS provider shall electronically notify the Disability Rights Office of the Federal Communications Commission's (Commission) Consumer and Governmental Affairs Bureau, the United States Secret Service (Secret Service), and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility on its website.

(1) A TRS provider shall, at a minimum, include in its notification to the Commission, Secret Service, and FBI:

(i) the TRS provider's address and contact information;

(ii) a description of the breach incident;

(iii) a description of the customer information that was used, disclosed, or accessed;

(iv) the method of compromise;

(v) the date range of the incident;

(vi) the approximate number of customers affected;

(vii) an estimate of financial loss to the provider and customers, if any; and

(viii) the types of data breached.

(2) If the Commission, or a law enforcement or national security agency notifies the TRS provider that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the TRS provider not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the TRS provider when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the TRS provider, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by TRS providers.

(3) A TRS provider is exempt from the requirement to provide notification to the Commission and law enforcement pursuant to paragraph (a) of this section of a breach that affects fewer than 500

customers and the carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. In circumstances where a carrier initially determined that it qualified for an exemption under this subsection, but later discovers information such that this exemption no longer applies, the carrier must report the breach to federal agencies as soon as practicable, but not later than within seven business days of this discovery, as required in paragraph (a).

(b) *Customer Notification.* Except as provided in paragraph (a)(2) of this section, a TRS provider shall notify affected customers of breaches of covered data without unreasonable delay after notification to the Commission and law enforcement as described in paragraph (a) of this section, and no later than 30 days after reasonable determination of a breach. This notification shall include sufficient information so as to make a reasonable customer aware that a breach occurred on a certain date, or within a certain estimated timeframe, and that such a breach affected or may have affected that customer's data. Notwithstanding the foregoing, customer notification shall not be required where a TRS provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach, or where the breach solely involves encrypted data and the provider has definitive evidence that the encryption key was not also accessed, used, or disclosed.

(c) *Recordkeeping.* A TRS provider shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the Commission, Secret Service, and the FBI pursuant to paragraph (a) of this section, and notifications made to customers pursuant to paragraph (b) of this section. The record shall include, if available, the dates of discovery and notification, a detailed description of the covered data that was the subject of the breach, the circumstances of the breach, and the bases of any determinations regarding the number of affected customers or likelihood of harm as a result of the breach. TRS providers shall retain the record for a minimum of 2 years.

(d) *Annual Reporting of Certain Small Breaches.* A TRS provider shall have an officer, as an agent of the provider, sign and file with the Commission, Secret Service, and FBI, a summary of all breaches occurring in the previous calendar year affecting fewer than 500 individuals and where the provider could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. This filing shall be made annually, on or before February 1 of each year, through the central reporting facility, for data pertaining to the previous calendar year.

(e) *Definitions.*

(1) As used in this section, a "breach" occurs when a person, without authorization or exceeding authorization, gains access to, uses, or discloses covered data. A "breach" shall not include a good-faith acquisition of covered data by an employee or agent of a TRS provider where such information is not used improperly or further disclosed.

(2) As used in this section, "covered data" includes (1) a customer's CPNI, as defined by section 64.5103 of this chapter; (2) personally identifiable information, as defined by section 64.2011(e)(5) of this chapter; and (3) the content of any relayed conversation within the meaning of § 64.604(a)(2)(i).

(3) As used in this section, "encrypted data" means covered data that has been transformed through the use of an algorithmic process into a form that is unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.

(4) As used in this section, "encryption key" means the confidential key or process designed to render encrypted data useable, readable, or decipherable.

* * * * *

APPENDIX B

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Data Breach Reporting Requirements* (*Data* Breach *Notice*), released in January 2023.[2] The Commission sought written public comment on the proposals in the *Data Breach Notice*, including comment on the IRFA. No comments were filed addressing the IRFA. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the *Report and Order*

2. The *Report and Order* takes several important steps aimed at updating the Commission's rules regarding data breach notifications, both to federal agencies and to customers, to better protect consumers from the dangers associated with data security breaches of customer information and to ensure that the Commission's rules keep pace with modern challenges.

3. First, the Commission expands the scope of the data breach notification rules to cover various categories of personally identifiable information (PII) that carriers hold with respect to their customers. Second, the Commission expands the definition of "breach" for telecommunications carriers[4] to include inadvertent access, use, or disclosure of customer information, except in those cases where such information is acquired in good faith by an employee or agent of a carrier, and such information is not used improperly or futher disclosed. Third, we require carriers to notify the Commission, in addition to the United States Secret Service (Secret Service) and Federal Bureau of Investigation (FBI), as soon as practicable, and in no event later than seven business days after reasonable determination of a breach. Fourth, we eliminate the requirement that carriers notify customers of a breach in cases where a carrier can reasonably determine that no harm to customers is reasonably likely to occur as a result of the breach, or where a breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed. Fifth, we eliminate the mandatory waiting period for carriers to notify customers, and instead requires carriers to notify customers of breaches of covered data without unreasonable delay after notification to federal agencies, and in no case more than 30 days following reasonable determination of a breach, unless a delay is requested by law enforcement. Sixth, and finally, to ensure that telecommunications relay service (TRS) customers enjoy the same level of protections as customers of telecommunications carriers, we adopt equivalent requirements for TRS providers. By adopting these requirements we increase the the protection of consumers from improper use and/or disclosure of their information consistent with approaches to protect the public adopted by our federal and state government partners.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

4. There were no comments raised that specifically addressed the proposed rules and policies

[1] 5 U.S.C. § 604. The RFA, 5 U.S.C. §§ 601–612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *See Data Breach Reporting Requirements*, WC Docket No. 22-21, Notice of Proposed Rulemaking, FCC 22-102 (2023) (*Data Breach Notice*).

[3] 5 U.S.C. § 604.

[4] As in the *Data Breach Notice*, in the *Report and Order* we refer to telecommunications carriers and interconnected VoIP providers collectively as "telecommunications carriers" or "carriers," consistent with our existing Part 64, Subpart U rules. *See Data Breach Notice,* at 3, para. 3 n.12. In doing so, the Commission does not address the regulatory classification of interconnected VoIP service or interconnected VoIP service providers. 47 CFR § 64.2003(o) (defining *telecommunications carrier* or *carrier* for purposes of Subpart U to include an entity that provides interconnected VoIP service as that term is defined in 47 CFR § 9.3).

presented in the IRFA. Nonetheless, the Commission considered the general comments received about the potential impact of the rules proposed in the IRFA on small entities and took steps where appropriate and feasible, as discussed below, to reduce the compliance burden and the economic impact of the rules adopted in the *Report and Order* on small entities.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

5. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[5] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply

6. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein.[6] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[7] In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act.[8] A "small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[9]

7. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[10] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[11] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.[12]

8. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[13] The

[5] 5 U.S.C. § 604(a)(3).

[6] *See id.* § 604(a)(4).

[7] *Id.* § 601(6).

[8] *Id.* § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register." *Id.*

[9] *See* 15 U.S.C. § 632.

[10] *See* 5 U.S.C. § 601(3)-(6).

[11] *See* SBA, Office of Advocacy, *Frequently Asked Questions, "What is a small business?"* (Mar. 2023), https://advocacy.sba.gov/wp-content/uploads/2023/03/Frequently-Asked-Questions-About-Small-Business-March-2023-508c.pdf.

[12] *Id*.

[13] *See* 5 U.S.C. § 601(4).

Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[14] Nationwide, for tax year 2020, there were approximately 447,689 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.[15]

9. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[16] U.S. Census Bureau data from the 2017 Census of Governments[17] indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[18] Of this number there were 36,931 general purpose governments (county[19], municipal and town or township[20]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[21] with enrollment

[14] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. *See* Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[15] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000, for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[16] *See* 5 U.S.C. § 601(5).

[17] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7." *See also* U.S. Census Bureau, *About Census of Governments*, https://www.census.gov/programs-surveys/cog/about.html (last updated Nov. 2021).

[18] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[19] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[20] *See id. at* tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[21] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

populations of less than 50,000.[22] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[23]

1. Wireline Carriers

10. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[24] Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband Internet services.[25] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[26] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[27]

11. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[28] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[29] Of this number, 2,964 firms operated with fewer than 250 employees.[30] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services.[31] Of these providers, the Commission estimates that 4,146

[22] While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[23] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments - Organizations tbls.5, 6 & 10.

[24] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[25] *Id.*

[26] *Id.*

[27] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[28] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[29] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[30] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[31] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

providers have 1,500 or fewer employees.[32] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

12. *Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers[33] is the closest industry with an SBA small business size standard.[34] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[35] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[36] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[37] Of this number, 2,964 firms operated with fewer than 250 employees.[38] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were fixed local exchange service providers.[39] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[40] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities. *Incumbent Local Exchange Carriers* (*Incumbent LECs*). Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers[41] is the closest industry with an SBA small business size standard.[42] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[43] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[44] Of this number, 2,964 firms

[32] *Id.*

[33] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[34] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[35] Fixed Local Exchange Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[36] *Id.*

[37] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[38] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[39] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[40] *Id.*

[41] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[42] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[43] *Id.*

[44] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

operated with fewer than 250 employees.[45] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers.[46] Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees.[47] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

13. *Incumbent Local Exchange Carriers (Incumbent LECs).* Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers[48] is the closest industry with an SBA small business size standard.[49] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[50] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[51] Of this number, 2,964 firms operated with fewer than 250 employees.[52] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers.[53] Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees.[54] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

14. *Competitive Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers.[55] Wired Telecommunications Carriers[56] is the closest industry with a SBA small business size standard.

---

[45] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[46] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[47] *Id.*

[48] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[49] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[50] *Id.*

[51] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[52] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[53] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[54] *Id.*

[55] Competitive Local Exchange Service Providers include the following types of providers: Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[56] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[57] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[58] Of this number, 2,964 firms operated with fewer than 250 employees.[59] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local exchange service providers.[60] Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees.[61] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

15. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[62] is the closest industry with a SBA small business size standard.[63] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[64] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[65] Of this number, 2,964 firms operated with fewer than 250 employees.[66] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or fewer employees.[67] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

16. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended, contains a size standard for a "small cable operator," which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[68] For purposes of the Telecom Act Standard, the Commission determined that a cable

[57] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[58] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[59] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[60] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[61] *Id.*

[62] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[63] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[64] *Id.*

[65] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[66] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[67] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[68] 47 U.S.C. § 543(m)(2).

system operator that serves fewer than 498,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator.[69] Based on industry data, only six cable system operators have more than 498,000 subscribers.[70] Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[71] Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

17. *Other Toll Carriers*. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers[72] is the closest industry with a SBA small business size standard.[73] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[74] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[75] Of this number, 2,964 firms operated with fewer than 250 employees.[76] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 90 providers that reported they were engaged in the provision of other toll services.[77] Of these providers, the Commission estimates that 87 providers have 1,500 or fewer employees.[78] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

2. Wireless Carriers

18. *Wireless Telecommunications Carriers (except Satellite*). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide

[69] *FCC Announces Updated Subscriber Threshold for the Definition of Small Cable Operator*, Public Notice, DA 23-906 (MB 2023) (*2023 Subscriber Threshold PN*). In this Public Notice, the Commission determined that there were approximately 49.8 million cable subscribers in the United States at that time using the most reliable source publicly available. *Id*. This threshold will remain in effect until the Commission issues a superseding Public Notice.. *See* 47 CFR § 76.901(e)(1).

[70] S&P Global Market Intelligence, S&P Capital IQ Pro, *Top Cable MSOs 06/23Q (*last visited Sept. 27, 2023); S&P Global Market Intelligence, Multichannel Video Subscriptions, Top 10 (April 2022).

[71] The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(e) of the Commission's rules. *See* 47 CFR § 76.910(b).

[72] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[73] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[74] *Id.*

[75] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[76] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[77] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

[78] *Id.*

communications via the airwaves.[79] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless Internet access, and wireless video services.[80] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[81] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[82] Of that number, 2,837 firms employed fewer than 250 employees.[83] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services.[84] Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees.[85] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

19. *Satellite Telecommunications.* This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications."[86] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small.[87] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[88] Of this number, 242 firms had revenue of less than $25 million.[89] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 65 providers that reported they were engaged in the provision of satellite telecommunications services.[90] Of these providers, the Commission estimates that approximately

[79] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[80] *Id.*

[81] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[82] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[83] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[84] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[85] *Id.*

[86] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[87] *See* 13 CFR § 121.201, NAICS Code 517410.

[88] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[89] *Id*. The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[90] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

42 providers have 1,500 or fewer employees.[91] Consequently, using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

3. Resellers

20. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with a SBA small business size standard.[92] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[93] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[94] Mobile virtual network operators (MVNOs) are included in this industry.[95] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[96] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[97] Of that number, 1,375 firms operated with fewer than 250 employees.[98] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported they were engaged in the provision of local resale services.[99] Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees.[100] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

21. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[101] is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[102] Mobile virtual network operators (MVNOs)

---

[91] *Id.*

[92] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[93] *Id.*

[94] *Id*.

[95] *Id*.

[96] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[97] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[98] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[99] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[100] *Id.*

[101] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[102] *Id.*

are included in this industry.[103] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[104] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[105] Of that number, 1,375 firms operated with fewer than 250 employees.[106] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 457 providers that reported they were engaged in the provision of toll services.[107] Of these providers, the Commission estimates that 438 providers have 1,500 or fewer employees.[108] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

22. *Prepaid Calling Card Providers*. Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. Telecommunications Resellers[109] is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[110] Mobile virtual network operators (MVNOs) are included in this industry.[111] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[112] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[113] Of that number, 1,375 firms operated with fewer than 250 employees.[114] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 62 providers that reported they were engaged in the provision of prepaid card services.[115] Of these providers, the Commission estimates that 61 providers have 1,500 or fewer

[103] *Id*.

[104] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[105] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[106] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[107] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

[108] *Id.*

[109] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[110] *Id.*

[111] *Id*.

[112] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[113] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[114] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[115] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022),

(continued….)

employees.[116] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities. Other Entities

23. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[117] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[118] Providers of Internet services (e.g. dial-up ISPs) or Voice over Internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[119] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[120] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[121] Of those firms, 1,039 had revenue of less than $25 million.[122] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

24. In the *Report and Order*, we expanded the scope of the Commission's breach notification rules to cover various categories of customer PII held by telecommunications carriers. We also adopted a requirement that all telecommunications carriers notify the Commission, in addition to the Secret Service and the FBI, as soon as practicable, and in no event later than seven business days after reasonable determination of a breach of covered data. We exempted from this notification requirement breaches that affect fewer than 500 customers and for which the carrier reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach. Instead, we required carriers to sign and file with the Commission and other law enforcement an annual summary regarding all such breaches occurring in the previous calendar year. Carriers must also notify affected customers of breaches, with the exception of instances where a carrier can reasonably determine that no harm to such customers is reasonably likely to occur as a result of the breach. Additionally, we applied similar rules to TRS providers.[123]

(Continued from previous page)
https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf. https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf

[116] *Id.*

[117] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[118] *Id.*

[119] *Id*.

[120] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[121] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[122] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[123] The breach notification and reporting obligations for TRS providers to covered data which includes TRS call content, includes customer PII and Customer Proprietary Network Information (CPNI).

25. Our review of the record included comments about unique burdens for small businesses that may be impacted by the notification requirements adopted in the *Report and Order*. Accordingly, the Commission considered, and adopted provisions to mitigate, some of those concerns. For example, the Commission decided to utilize the existing reporting portal, which small and other carriers and TRS providers are already accustomed to using to notify the Commission along with the Secret Service and FBI of breaches rather than creating a centralized reporting facility operated by the Commission to report breaches to the Commission and these agencies as proposed in the *Data Breach Notice*. As such, the Commission anticipates that the requirement to notify it of data breaches will have de minimis cost implications because small and other carriers and TRS providers are already obligated to notify the Secret Service and FBI of such breaches, and will use the existing portal to do so. The Commission delegated authority to the Wireline Competition Bureau to coordinate with the Secret Service, the current administrator of the reporting facility, and the FBI, to the extent necessary, to ensure that the Commission will be notified when data breaches are reported, thereby ensuring that no additional burden would be imposed on small and other carriers and TRS providers. The Commission also adopted a threshold trigger that permits carriers and TRS providers to forgo notifying federal agencies of breaches that are limited in scope and unlikely to pose harm to customers, instead requiring small and other carriers and TRS providers to maintain the information, and file an annual summary of such breaches. Additionally, with the support of several small carriers, the Commission adopted a harm-based notification trigger for reporting breaches to customers, which allows small and rural providers to focus their resources on data security and mitigation measures rather than generating notifications where harm to the consumer is unlikely.[124]

26. In the *Report and Order* we also adopted a "without unreasonable delay, but no later than 30 days after reasonable determination of the breach" timeframe for notifying customers of covered data breaches. Consistent with the comments in support of small carriers interests, we recognize that this reporting standard can take into account factors such as the provider's size, as a small carrier may have limited resources and could require additional time to investigate a data breach than a large carrier.[125] We note that many state laws similarly require breach notifications which are in line with the requirements that the Commission adopts today. Therefore, although the Commission cannot quantify the compliance costs, we do not expect the adopted rules to impose any significant cost burdens for small entities, or require these entities to hire professionals to meet their compliance obligations.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

27. The RFA requires an agency to provide "a description of the steps the agency has taken to minimize the significant economic impact on small entities . . . including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[126]

28. The Commission took steps and considered alternatives in this proceeding that may reduce the impact of the adopted rule changes on small entities. For example, our expansion of the definition of "breach" included consideration of whether to include situations where a telecommunications carrier, or a third party discovers conduct that could have reasonably led to exposure

[124] Blooston Rural Carriers Comments at 2; WISPA Comments at 5.

[125] ACA Connects Comments at 14; Blooston Rural Carriers Comments at 5-6; Blooston Rural Carriers Reply at 3 ("A reasonableness timeframe will allow service providers to respond more quickly when circumstances warrant, while at the same time allowing flexibility if a small service provider has limited personnel and/or resources available and is focused on addressing and minimizing harm to consumers.").

[126] 5 U.S.C. § 604(a)(6).

of customer CPNI, even if it has not yet determined if such exposure occurred.[127] Small and other commenters generally opposed such an expansion,[128] and we ultimately declined to expand "breach" to include these situations. Conversely, although some commenters on behalf of small entities opposed requiring breach notification to the Commission, we were not persuaded by their arguments.[129] We disagreed that the existing requirement to notify the Secret Service and the FBI is sufficient and that adding the Commission to the list of recipients of the same breach notifications Commission rules already require carriers to submit would impose any additional burden on carriers. Several actions we take in the *Report and Order* will avoid imposing additional burdens on small and other carriers who have to file breach notifications with the Commission.

29. As an initial matter the Commission considered, and included a good-faith exception that excluded from the definition of "breach" a good-faith acquisition of covered data by an employee or agent of a carrier where such information is not used improperly or further disclosed.[130] We believe this exception will help avoid excessive notifications to consumers, and reduce reporting burdens on small and other carriers.[131] Furthermore, in the *Data Breach Notice*, the Commission proposed to create a new portal for reporting breaches to the Commission. However, in the *Report and Order* we decided instead to make use of the existing portal which small and other carriers and TRS providers are already accustomed to using for data breach reporting requirements to federal law enforcement agencies. Our decision to continue using a portal that small and other carriers and providers are already familiar and comfortable working with reduces the administrative burdens on small entities of learning a new mechanism and creating new reporting processes. Additionally, the contents of the notification to the Commission are the same fields that carriers and providers already report to the Secret Service and the FBI. We agreed with commenters on behalf of small entities that the breach notification information small and other carriers and providers are required to submit to the FBI and Secret Service is largely sufficient, and the Commission should generally require reporting of the same information.[132] As such, the impact of also reporting the breach to the Commission should be de minimis on small carriers and providers. The Commission considered adopting a lower reporting threshold for the affected-customer notification of no-harm-risk breaches to the federal agencies but ultimately decided to adopt a 500-

[127] *Data Breach Notice* at 10, para. 14.

[128] ACA Connects Comments at 4-5 n.10; USTelecom Comments at 5-6; WISPA Comments at 4; CTIA Comments at 27; Verizon Comments at 9-10; WTA Reply at 2 (contending that "conduct or security weaknesses that theoretically or potentially could have led to exposure of CPNI (but where there is no evidence that they actually did) are matters for carrier corrective actions and employee training . . .").

[129] WISPA Comments at 6.

[130] *Data Breach Notice* at 9, para. 14. In the *Data Breach Notice*, we used the term "exemption" instead of "exception" when asking commenters whether we should exclude from the definition of "breach" a good-faith acquisition of covered data. *See id.* at 10, para. 14. For the purpose of clarity, we instead use the word "exception" here to describe this exclusion. While we make this exception to our definition of "breach," we nevertheless expect carriers to "take reasonable measures" in such scenarios to protect such customer information from improper use or further disclosure, which may, for example, involve requiring that such an employee or agent destroy the data upon realizing that the data was disclosed without, or in excess of, authorization. *Cf.* 47 CFR § 64.2010(a) (requiring telecommunications carriers to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI).

[131] Blooston Rural Carriers Comments at 2 (Arguing that a good-faith exception will prevent carriers from "unnecessarily confus[ing] and alarm[ing] consumers" in such low-risk situations); National Rural Electric Cooperative Association (NRECA) Reply at 4 (Arguing that without the exception, "more serious data breaches [will potentially] become lost in the 'noise' of multiple notifications.")

[132] WISPA Comments at 7 (Arguing that "the information currently submitted through the FBI/Secret Service reporting facility is largely sufficient and that generally the same information should be reported" under the Commission's updated rules).

customer threshold because that is consistent with many other state laws, and would therefore promote consistency and efficiency in compliance. A lower threshold could impose higher burdens on small and other carriers and providers, so we declined to adopt such a rule. Likewise for consistency and efficiency, we similarly declined to adopt a threshold of 5000 affected customers to trigger notification to federal agencies.[133] The Commission also considered ways to reduce the burden of the annual reporting requirement for breaches affecting fewer than 500 individuals and where the carrier or TRS provider could reasonably determine that no harm to customers was reasonably likely to occur as a result of the breach. In determining the content and format requirements of the annual report, the Commission instructed the Bureau to minimize the burdens on carriers and TRS providers by, for example, limiting the content required for each reported breach to that absolutely necessary to identify patterns or gaps that require further Commission inquiry. At a minimum, the Commission directed the Bureau to develop requirements that are less burdensome than what is required for individual breach submissions to the reporting facility, and to consider streamlined ways for filers to report this summary information.

30. The Commission also considered adopting minimum requirements for the contents of customer notifications for telecommunications carriers and TRS providers. However, we declined to impose such minimum requirements on carriers and TRS providers because doing so may create unnecessary burdens on carriers and TRS providers, particularly small ones. Specifically, we considered but declined to adopt minimum reporting requirements harmonizing content requirements for carriers with the information required under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) as part of their notifications to federal agencies.[134] In the absence of final rules, and a potential for imposing duplicative or inconsistent fields,[135] by declining to adopt such a requirement we minimize the economic impact for small entities. Relatedly, we declined to adopt a specific method of notification for customers, instead deciding that carriers and TRS providers have pre-established methods of reaching their customers, each carrier or TRS provider is in the best position to know how best to reach their customers, and imposing a specific method would add unnecessary burdens to the industry. The Commission also considered requiring notification to all customers whenever a breach occurred. Such a requirement would lead to increased obligations to notify customers of every instance which qualified as a "breach" under the expanded definition and scope of the rules described in the *Report and Order*. However, by adopting the harm-based trigger, we limit the applicability of the customer-notification obligations to breaches which are likely to cause harm to customers, thereby reducing burdens on small and other telecommunications carriers and TRS providers. In addition, we also adopted a safe harbor under which customer notification is not required where a breach solely involves encrypted data and the carrier has definitive evidence that the encryption key was not also accessed, used, or disclosed, further reducing burdens on small and other carriers from the Commission's customer notification requirements.

31. The Commission's actions and the considerations discussed above lead us to believe that the new requirements adopted in the *Report and Order* are minimally burdensome, and small carriers and

[133] WTA Comments at 7; Blooston Rural Carriers Reply at 5.

[134] *Data Breach Notice* at 14, para. 27.

[135] ACA Connects Comments at 9-10 n.23 ("[A]t this juncture there is no way for the Commission to predict with any certainty whether, and if so to what degree, any revised data breach notification rules the Commission adopts would align with those ultimately adopted by CISA. . . . [T]he substance of the eventual CISA rules is too speculative for the Commission to consider harmonizing its data breach notification rules with CISA's cyber incident reporting rules at this time. Once both agencies adopt their respective incident notification rules, the Commission may further evaluate how to minimize potential duplicate reporting of CPNI breaches arising from cyber incidents, for instance by carving out reporting under the Commission's rules in favor of reporting to CISA where the incident is cyber-based."); Blooston Rural Carriers Comments at 4 (advocating for coordination of our data breach reporting requirements with the CISA "once data breach reporting under the recently-passed [CIRCIA] is in place"); CCA Comments at 3-4 ("The Commission should refrain from needlessly duplicating cyber incident reporting requirements currently being implemented by the [CISA].").

TRS providers should not have any increased regulatory burdens, or significant compliance issues with including these new breach notification requirements in their existing processes. Nevertheless, the importance of the breach notification requirements adopted in the *Report and Order* to safeguard the public against improper use or disclosure of their customer data, to hold telecommunications carriers and TRS providers accountable, and to ensure customers are provided with the necessary resources to protect themselves in the event their data through their association with a telecommunications carrier or TRS provider is compromised, outweighs any minimal burdens that telecommunications carriers and TRS providers may experience in providing information to the Commission, and federal law enforcement agencies.

G. Report to Congress

32. The Commission will send a copy of the *Report and Order*, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act.[136] In addition, the Commission will send a copy of the *Report and Order*, including this FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the *Report and Order* (or summaries thereof) will also be published in the Federal Register.[137]

[136] *Id.* § 801(a)(1)(A).

[137] *See id*. § 604(b).

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Data Breach Reporting Requirements*, WC Docket No. 22-21, Report and Order (December 13, 2023)

It has been sixteen years since the Federal Communications Commission last updated its policies to protect consumers from data breaches. Sixteen years! To be clear, that was before the iPhone was introduced. There were no smart phones, there was no app store, there were no blue and green bubbles for text. It was a long time ago. In the intervening years a lot has changed about when, where, and how we use our phones, and what data our providers collect about us when we do. But not the FCC's data breach rules; they remain stuck in the analog age.

Today we fix this problem. We update our policies to protect consumers from digital age data breaches. We make clear that under the Communications Act carriers have a duty to protect the privacy and security of consumer data.

First, we modernize our data breach rules to make clear they include all personally identifiable information. In the past, these rules have only prohibited the disclosure of information about who we call and when. But consumers also deserve to know if their carrier has disclosed their social security number or financial data or other sensitive information that could put them in harm's way. We fix that today—and it is overdue.

Second, we modernize our data breach rules to make clear they cover intentional and inadvertent disclosure of customer information. Consumers deserve protection regardless of whether the release of their personally identifiable information was intentional or accidental. Either way, they could find themselves in trouble, so our rules need to address both.

Third, we modernize our standards for notification. That means in the event of a data breach, your carrier has to tell the FCC and tell you in a timely way just what happened and what personal information may be at risk. Our old rules required carriers to wait seven business days before telling consumers what breaches had taken place. But there is no reason why consumers should have to wait that long before learning that their personal information has been stolen or misused.

Finally, we update reporting requirements associated with data breaches. We also make clear our policies apply to telecommunications relay service providers, so that those with disabilities get the same protections as everyone else.

These are necessary updates. Find a consumer with a phone anywhere and they would tell you every one of these changes make sense. What makes no sense is leaving our policies stuck in the analog era. Our phones now know so much about where we go and who we are, we need rules on the books that make sure carriers keep our information safe and cybersecure.

I want to thank the Commission's Privacy and Data Protection Task Force for their input into this effort and work to update our privacy and security policies across the board. I also want to note that with the help of the task force, for the first time ever the FCC has signed Memoranda of Understanding with Attorneys General from Pennsylvania, Illinois, Connecticut, and New York who are committing to work with us on privacy, data protection, and cybersecurity enforcement matters.

A thank you also goes to our colleagues at the U.S. Secret Service and Federal Bureau of Investigation for their input and support on this effort. Let me also commend staff at the agency for their work, including Callie Coker, Adam Copeland, Trent Harkrader, Melissa Kirkel, Jodie May, Kimia Nikseresht, Zach Ross, Mason Shefa, and John Visclosky from the Wireline Competition Bureau; Robert

Aldrich, Diane Burstein, Aaron Garza, Eliot Greenwald, Ike Ofobike, Alejandro Roark, Michael Scott, and Mark Stone from the Consumer and Governmental Affairs Bureau; Maureen Bizhko, John Blumenschein, Justin Cain, Michael Connelly, Debra Jordan, Nicole McGinnis, Erika Olsen, Austin Randazzo, and Chris Smeenk from the Public Safety and Homeland Security Bureau; Hunter Deeley, Loyaan Egal, Peter Hyun, Ryan McDonald, Victoria Randazzo, Phillip Rosario, Kristi Thompson, and Shana Yates from the Enforcement Bureau; Barbara Esbin, Garnet Hanly, and John Lockwood from the Wireless Telecommunications Bureau; Michael Janson, Douglas Klein, Marcus Maher, Richard Mallen, Royce Sherlock, Anjali Singh, and Elliot Tarloff from the Office of General Counsel; Mark Azic, Eugene Kiselev, Giulia McHenry, and Steven Rosenberg from the Office of Economics and Analytics; and Joy Ragsdale and Chana Wilkerson from the Office of Communications Business Opportunities.

DISSENTING STATEMENT OF COMMISSIONER BRENDAN CARR

Re: *Data Breach Reporting Requirements*, Report and Order, WC Docket No. 22-21.

In 2016, the FCC adopted a data breach notification rule in a partisan, 3-2 decision. In 2017, the House, the Senate, and the President all came together and nullified that rule by passing a joint resolution of disapproval under the Congressional Review Act (CRA). It was a rare rebuke of an agency rule. Indeed, in the 27 years since Congress enacted the CRA, the law has only been used 20 times. It is strong medicine, too. When a President signs a CRA into a law, it not only prohibits an agency from readopting the relevant rule, it also prohibits the agency from enacting a substantially similar rule in the future without specific legislative authorization from Congress. In other words, when an agency earns the distinction of having a rule nullified by the CRA, the Legislative Branch and Executive Branch are joining together to take back the agency's rulemaking authority in the relevant area and, going forward, future regulation, if any, must come from Congress itself. As a constitutional matter, administrative agencies have an obligation to abide by these decisions.

Yet today, the Commission makes no real attempt to explain how the data breach rule we adopt today is not the same or substantially similar to the one nullified by the House, the Senate, and the President in the 2017 CRA.[1] This plainly violates the law.

The FCC's only real defense is one that reads the CRA out of the United States Code altogether. The Order notes that the 2016 FCC decision adopted several rules—all of which were nullified by the 2017 CRA. But in the Order's view, the CRA does not prohibit the FCC from putting any one of those rules (or even some combination of them) back in place here provided that the FCC does not put all of those 2016 rules back in place in this one decision. This creates an exception that swallows the CRA whole. Indeed, if the FCC's theory were correct, then agencies could insulate any one of their rules from the CRA (no matter how strongly the House, the Senate, and the President felt about the rule) simply by packaging that one rule together with other rules in a single document. Then, under the FCC's theory, the agency could always put that one rule back in place, provided it did not reenact those other rules that the agency packaged along with it. This is a sweeping theory that far exceeds the limits that the Legislative Branch and the Executive Branch have placed on agency decision making. Indeed, in a letter to the FCC this week, leaders in the Senate warned that the Commission's interpretation "would eviscerate the CRA".[2]

But the FCC's decision today violates more than the CRA. It also violates the APA. In the Notice of Proposed Rulemaking (NPRM) that launched this proceeding, the Commission expressly stated, in negotiated language, that the agency was not seeking comment on putting back in place or otherwise issuing a new rule that is the same as or substantially similar to the rule disapproved by Congress in 2017. Yet that is exactly what the FCC chooses to do with this data breach rule. Thus, while some have argued that any FCC violation of the CRA is unreviewable by the courts, an FCC violation of the APA is always reviewable.

[1] Through a set of late-round edits, the Order suggests that there are a couple of ways that this data breach rule may be different from the 2016 data breach rule. But the changes highlighted by the Order in this respect are not of the type or substance that would be necessary for this 2023 rule to fall outside the reach of the 2017 CRA.

[2] Letter from Sen. Ted Cruz, Ranking Member, Senate Committee on Commerce, Science, and Technology, et al., to Hon. Jessica Rosenworcel, Chair, FCC (Dec. 12, 2023) (stating the FCC "is defying clear and specific direction not to issue requirements that are substantially similar to parts of a rule disapproved by Congress." on behalf of 4 U.S. Senators).

The Order's problems only compound from there. Indeed, even if the CRA never passed, the FCC's decision would exceed the Commission's authority. For instance, instead of limiting the FCC's rule to the set of customer proprietary network information (CPNI) over which the agency has jurisdiction, the Order purports to expand the agency's CPNI framework to an expansive set of personally identifiable information (PII)—even though Congress never gave us authority to regulate PII in this manner and the Commission never sought comment on doing so.

In the end, the agency could have proceeded with a set of rules based on the NPRM that would have made progress on data breach issues while staying within the clear bounds Congress set on FCC action. However, I cannot support this expansive interpretation of the Commission's authority—especially in light of the clear constraints that the House, the Senate, and the President imposed on the agency through the 2017 CRA. Accordingly, I dissent.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Data Breach Reporting Requirements*, WC Docket No. 22-21, Report and Order

Unfortunately, we've all been there. You check your mail only to find a letter from a service provider announcing that your sensitive information has been leaked as part of a data breach. And, if it seems like these notifications and announcements are happening more frequently, you're right. According to a recent report, data breaches impacting US organizations are already at an all-time high. There were more breaches in the first three quarters of 2023 than in any prior year.[1] Another report states that the United States saw 1,802 data breaches in 2022 with 422.14 million records exposed and 298 million Americans impacted.[2]

This matters. Sensitive data breaches include the type of information that bad actors can exploit for identify theft, financial fraud and crimes, and scams, placing consumers at risk in a multitude of ways.

Congress recognized this too. Section 222 of the Communications Act gives us clear authority, and carriers a duty, to protect the confidentiality of proprietary information of and relating to consumers and others.[3] We first adopted our data breach rules 16 years ago in 2007, but the intervening years have shown that our data breach rules are badly in need of an update. The amount of data service providers now collect and retain has greatly expanded the risk profile for consumers and their carriers, as does the sophistication of bad actors who are constantly trying to access that data. So, I'm glad that we update our rules today in response to the reality that we need to do more to both protect sensitive consumer data and notify consumers and the authorities when a data breach occurs.

One overdue change is to properly expand the definition of "breach" beyond the intentional access, use, or disclosure of covered data. Many breaches are inadvertent, but harmful nonetheless, and the impact on consumers when their data is disclosed does not turn on the question of intent. At the same time, we recognize that breach notice fatigue is real. To avoid this risk, the Order properly adopts a harm-based notification trigger and an affected consumer trigger threshold that limits the consumer reporting requirement and balances the need for notice with the burden on consumers if harm is unlikely. We should also continue to work with our agency partners to coordinate filing obligations across the government over time, including as the Cybersecurity and Information Security Agency works on their Cybersecurity Incident Reporting rulemaking.

I also agree with the need for providers to encrypt their data, especially sensitive data. I can't emphasize it enough—at a minimum, providers should be encrypting the data they hold as a basic best practice. While we do not require encryption in this item, we adopt encryption as a safe harbor, recognizing it is a critical defense against data breaches and incentivizing providers to embrace it. Consumers trust providers with their most sensitive information, and the marketplace demands that carriers take these widely available steps to protect them, including measures like access controls, firewalls, intrusion detection and prevention, and security audits and updates to further defend against modern cyber threats.

---

[1] Stuart E. Madnick, Ph.D., *The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase*, Dec. 2023, https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

[2] Ani Petrosyan, *Annual number of data compromises and individuals impacted in the United States from 2005 to 2022*, Statista Aug. 29, 2023, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[3] *See* 47 U.S.C. § 222(a).

I thank the Chairwoman for working with me on the edits that I suggested to help the item strike the right balance in defining the Personally Identifiable Information (PII) data that needs to be protected and the level of harm that triggers a reporting obligation. Data breaches will continue to be a problem, but by notifying consumers and the government we can take steps to mitigate the harm. I thank the Chairwoman for her leadership in updating our data breach rules and I thank the Commission staff for their hard work on this item. I approve.

DISSENTING STATEMENT OF
COMMISSIONER NATHAN SIMINGTON

Re: *In the Matter of Data Breach Reporting Requirements*, WC Docket No. 22-21

My primary objection to the order we adopt today is not that it is necessarily bad policy—even though it could benefit from greater clarity and specificity, as well as better targeting—but that it is part of an effort to nullify the 2017 Congressional Review Act resolution that overturned the *2016 Privacy Order*, which this order reimplements various provisions of.

The CRA prohibits an agency from adopting a rule that is "substantially the same" as a previous rule that was overturned by a CRA resolution. A wooden reading of the statute—that an order does not reissue "substantially the same" rule unless the individual order has almost all of the same provisions of the overturned rule—would turn the CRA's prohibition into a nullity. An agency seeking to circumvent a previous CRA resolution could just split the desired regulations into several orders and pass it piecemeal. To give the CRA meaningful effect, we must look at not just the content of any one order, but the totality of related orders adopted subsequent to a CRA resolution.

Readopting the *2016 Privacy Order* in piecemeal is exactly what the Commission is doing. Today, we adopt a breach notification rule for Title II providers, which right now, mostly means telephone companies. But two months ago, this Commission began the process of reclassifying broadband as a Title II service, which when complete, will subject broadband providers to these new rules as well, just as the 2016 order did. Last month, we adopted data security, customer authentication, employee training, and other requirements that mirror provisions of the 2016 order.[1] And I have no doubt that this Commission will, if given the chance, adopt even more aspects of the 2016 order.

In a further similarity, the order we adopt today dramatically expands the kinds of data that the FCC has jurisdiction over, exactly like the *2016 Privacy Order*. And it relies on the same dubious legal theory as the 2016 order. Traditionally, the FCC's privacy authority has been limited to "Customer Proprietary Network Information" (CPNI), a term of art defined and used in Section 222's grants of authority. CPNI is limited to " quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service." The majority is not satisfied with jurisdiction over only this data, and instead asserts jurisdiction over all personally identifiable information (PII). To justify this, it relies on the omission of the word "network" from the introductory sentence at Section 222(a). But this interpretation is inconsistent with decades of FCC interpretation and practice. The best interpretation of Section 222(a) is that it is not an independent source of authority, but a high-level summary of the more specific provisions that follow it.

[1] The majority argues that the requirements imposed by our *SIM Swap Order* are substantially different from similar requirements in the 2016 order because they are motivated by the prevention of SIM swap and port-out fraud, while the 2016 order was motivated by more general privacy and data security concerns. But the purposes which motivate our rulemakings are irrelevant, and only the actual scope of the adopted rules matters. The *SIM Swap Order* requires that "employees who receive inbound customer communications" be unable to access CPNI until the customer has been "properly authenticated." Nothing about this requirement is limited to the prevention of SIM swap or port-out fraud, and it is very similar to the 2016 order's requirement for providers to "take reasonable measures to secure PI," which was accompanied by a list of practices the FCC deemed "exemplary of reasonable data security" that included "robust customer authentication." And while other elements of the *SIM Swap Order*, like employee training and customer notification requirements, are in fact limited to SIM swap and port-out procedures, they nonetheless mirror employee training and customer notification requirements in the 2016 order. Taken with this order today and likely future Commission action, this looks like exactly the kind of piecemeal readoption of the *2016 Privacy Order* that I am concerned is underway.

With this order today, has the Commission reissued "substantially the same" rule as the 2016 Privacy Order? Quite possibly. And I am sure that this item is at least a major step toward doing that, which I cannot support. Therefore, I must dissent.

STATEMENT OF
COMMISSIONER ANNA M. GOMEZ

Re: *Data Breach Reporting Requirements*, WC Docket No. 22-21, Report and Order (December 13, 2023).

Nearly a decade ago, a unanimous Supreme Court noted that "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[1] Since 2014, the importance of mobile phones in our daily lives has only increased, and the data at risk has only become more sensitive. The sheer breadth and depth of information collected and stored by these devices underscore the increasing privacy and sensitivity of our digital footprints. As consumers rely more heavily on cell phones for daily activities, consumers expect that telecommunications providers will safeguard this sensitive data and their networks.

It is more than timely that we take a look at the Commission's existing data breach notification rules, and modernize them, where appropriate, aligning with the evolving landscape of cybersecurity threats. At the same time, we must be sure that in updating our rules and protecting consumers, we are striking the right balance of cost and benefit to implementing additional obligations on providers. We must be sure that our updates are intentional, and most importantly, that they benefit consumers.

To that extent, I am grateful to the stakeholders who have come in on this item and the discussions we've had on modernizing the data breach rules. We've made progress to ensure that these updates strike that balance between protecting consumers and refraining from imposing unnecessary burdens on providers. I thank the Chairwoman for taking my suggestions to reduce burdens on providers, while also maintaining strong safeguards to protect consumers. To the Wireline Competition Bureau, and the Public Safety and Homeland Security Bureau, thank you for your tireless work on this item.

[1] *Riley v. California*, 573 U.S. 373, 403 (2014).